Inventarisatie cybersecurity laadinfrastructuur

Eindrapportage

29 april 2021

management consultants

Management summary

Binnen de Nationale Agenda Laadinfrastructuur (NAL) werken overheden, onderzoeksinstellingen en marktpartijen samen aan de uitrol van de laadinfrastructuur die nodig is om de doelstellingen voor elektrisch vervoer in het Nederlands Klimaatakkoord te halen. Digitale veiligheid van de laadinfrastructuur is daarbij een belangrijk thema. In opdracht van de Taakgroep Cyber Security is een inventarisatie gedaan naar de stand van zaken van de cybersecurity van de bestaande laadinfrastructuur in Nederland, door middel van een online survey en verdiepende interviews onder Charge Point Operators (CPO's), laadpaalleveranciers en publieke opdrachtgevers.

Om het onderzoek af te bakenen is een toetskader opgesteld. Er is gekeken naar het laadstation, de digitale verbindingen hiermee en de organisatie waarbinnen de digitale beveiliging is belegd. Ondanks de beperkte respons op de online survey, dekt de inventarisatie ongeveer 70% van de publiek toegankelijke laadinfrastructuur en in mindere mate de semi-publiek en privaat toegankelijke laadinfrastructuur in Nederland. De survey-resultaten zijn verrijkt door het houden van verdiepende interviews met (deels) dezelfde partijen.

De resultaten tonen aan dat partijen zich bewust zijn van het belang van cybersecurity. Echter, dit bewustzijn is in veel gevallen gebaseerd op vertrouwen en niet altijd op expliciete afspraken aangaande de digitale veiligheid. Er dient duidelijkheid te komen wie welke rol en verantwoordelijkheid heeft in de keten ten aanzien van cybersecurity. Dit om te voorkomen dat de gedeelde verantwoordelijkheid ervoor zorgt dat uiteindelijk cybersecurity nergens is belegd. Om dit te bewerkstelligen dient er allereerst inzicht gecreëerd te worden in de risico's, impact en passende richtlijnen. Marktpartijen regelen dit het liefst op Europees niveau, ook gezien de internationale markten waarin zij opereren. De inspanningen in Nederland om te zorgen dat de uitrol van 1,9 miljoen laadpunten die nodig zijn in 2030 veilig gebeurt, moeten daarom parallel lopen met de inspanningen om hier op Europees niveau uniforme afspraken over te maken.

Within the National Agenda for Charging Infrastructure (NAL) governments, research and knowledge institutes and market parties work together on the roll-out of charging infrastructure. This is necessary to achieve the aims that have been set for sustainable transport in the National Climate Agreement. An important topic is the digital security, also known as cybersecurity, of the charging infrastructure. On behalf of the Taskforce Cyber Security an inventory has been conducted on the cybersecurity of current charging infrastructure in the Netherlands. Data was via an online survey and in-depth interviews with Charge Point Operators (CPO's), charge station suppliers and governments who procure charging infrastructure.

A framework has been drawn up to define the scope of the inventory. The scope includes the charging station, its digital connections and the organization surrounding the digital environment. Despite the limited response to the survey, the inventory covers approximately 70% of the Dutch public charging stations and to a lesser extent the semi-public and private charging stations. The results of the survey have been enriched by conducting interviews with (partly) the same stakeholders.

The results show that parties are aware of the importance of cybersecurity. However, in many cases this awareness is mainly based on trust and not on explicit agreements regarding cybersecurity. It is important to provide clarity about who fulfills what role in the chain of cybersecurity. This should ensure that the shared responsibility does not result in the fact that cybersecurity is not covered by any of the parties. To accomplish this, insight has to be gained in the risks, impact and fitting guidelines. Market parties prefer to organize this on a European level given the international markets in which they operate. The effort to ensure that the roll-out of 1.9 million charging points up to 2030 happens safely, should run in parallel with the effort to come to uniform agreements on a European level.

INHOUDSOPGAVE

Definities

AC	Alternating Current (wisselstroom)
CISO	Chief Information Security Officer, verantwoordelijk voor het implementeren van informatiebeveiligingsbeleid en het toezicht daarop.
CPO	Charge Point Operator
CSMS	Charge Station Management Systeem, het beheersysteem voor laadstations van de CPO.
DC	Direct Current (gelijkstroom)
Eichrecht	Duitse regeling die, ter bescherming van de consument, garandeert dat de stroom die in rekening wordt gebracht ook daadwerkelijk is geleverd door het laadstation.
EMS	Energie Management Systeem
eMSP	E-Mobility Service Provider
EV	Elektrisch voertuig
EV-rijder	Bestuurder van een EV
ISO 15118	Een internationale standaard die digitale communicatie tussen het voertuig en het laadstation mogelijk maakt.
Laadlocatie	Een locatie met één of meer laadstations met daarbij behorende laadplekken.
Laadpaalleverancier	Fabrikant die laadstations produceert en levert aan de markt.
Laadpunt	De elektrische energie wordt geleverd via een laadpunt, de elektrische aansluiting op een laadstation.
Laadstation	Een laadstation is een fysiek object met één of meerdere laadpunten. De interface op het laadstation kan bestaan uit een status led of display, toetsen en een betaalpas/RFID-lezer.
MFA	Multifactor-Authenticatie, een beveiliging waarbij de authenticatie met minimaal twee verschillende middelen wordt afgedwongen, bv. door een pas mèt pincode.
NKL	Nationaal Kennisplatform Laadinfrastructuur
OCPP	Open Charge Point Protocol is een protocol dat de communicatie beschrijft van de verbinding tussen het laadstation en het CSMS.
OEM	Original Equipment Manufacturer
Publiek toegankelijk laadstation	Een laadstation voor een elektrisch voertuig dat 24/7 openbaar toegankelijk is, zonder barrières zoals slagbomen of poorten.
Publieke opdrachtgever	Overheid die via een aanbesteding opdracht geeft voor de plaatsing van laadinfrastructuur.
Privaat toegankelijk laadstation	Een laadstation op eigen terrein bij een bedrijf of hotel. Het laadstation is doorgaans niet toegankelijk voor derden, maar het is mogelijk om het private laadstation beschikbaar te stellen voor gebruik door derden.
RFID	Radio Frequency IDentification, een technologie om op kleine afstand informatie te lezen van tokens of laadpassen.
SaaS	Software as a Service, software die niet als product wordt aangeschaft, maar als dienst wordt afgenomen. De aanbieder voert het onderhoud en beheer uit.

Semi-publiek toegankelijk laadstation	Een laadstation op een private locatie dat in meer, of mindere, mate is opengesteld voor publiek (bv. in parkeergarages, bij tankstations of retail- en horecalocaties). Er kunnen beperkingen gelden qua toegangstijden en bijvoorbeeld de vereiste om bepaalde producten/diensten af te nemen.
Thuislaadstation	Een laadstation op eigen terrein bij een woning. Het laadstation is doorgaans niet toegankelijk voor derden, maar het is mogelijk om het private laadstation beschikbaar te stellen voor gebruik door derden.

1. Inleiding

Binnen de Nationale Agenda Laadinfrastructuur (hierna: NAL) werken overheden, onderzoeksinstellingen en marktpartijen samen aan de uitrol van de laadinfrastructuur die nodig is om de doelstellingen voor elektrisch vervoer in het Nederlands Klimaatakkoord te halen. Veiligheid is daarbij een belangrijk thema om belemmeringen bij de opschaling van elektrisch vervoer te voorkomen. Het gaat daarbij zowel om de fysieke als digitale veiligheid van de laadinfrastructuur.

De Werkgroep Veiligheid draagt bij aan het veilig gebruiken en opladen van elektrische voertuigen. Binnen de werkgroep is de Taakgroep Cyber Security verantwoordelijk voor de digitale veiligheid. De taakgroep richt zich onder andere op het identificeren van risico's, het opstellen van maatregelen om cybersecurity te verbeteren en de borging hiervan via onder andere beleidsadviezen en bewustwording.

Voor de werkzaamheden van de Taakgroep Cyber Security is het van belang om allereerst inzicht te verkrijgen in de huidige stand van zaken van de cybersecurity van laadinfrastructuur. Het belang van dit inzicht wordt onderstreept door gestelde Kamervragen over de wijze waarop cybersecurity in Nederland is geborgd[1]. In opdracht van de taakgroep is door APPM een inventarisatie gedaan naar de stand van zaken van de cybersecurity van de bestaande laadinfrastructuur in Nederland, door middel van zowel een kwantitatief als kwalitatief onderzoek bestaande uit een online survey en verdiepende interviews onder Charge Point Operators (CPO's), laadpaalleveranciers en publieke opdrachtgevers. Voorliggend document betreft de eindrapportage van deze inventarisatie.

1.1 Leeswijzer

Hoofdstuk 2 beschrijft de aanpak van de studie en de afbakening hiervan middels een toetskader. In hoofdstuk 3 worden de resultaten gepresenteerd, ingedeeld naar de onderdelen van dit toetskader. Het rapport sluit af met de conclusie en aanbevelingen in hoofdstuk 4.

[1] Op 11 november 2020 zijn in de Tweede Kamer vragen gesteld over cybersecurity, zie ook https://zoek.officielebekendmakingen.nl/ah-tk-20202021-1414.html

2. Aanpak

In voorliggend hoofdstuk wordt beschreven welke aanpak gehanteerd is bij de inventarisatie naar de cybersecurity van laadinfrastructuur. De volgende paragrafen gaan in op de afbakening van de studie, de gebruikte methode en het opgestelde toetskader.

2.1 Algemene uitgangspunten

Een inventarisatie van de stand van zaken van de digitale beveiliging van laadinfrastructuur vraagt om een eenduidig beeld wat wordt geïnventariseerd. Om deze reden zijn in afstemming met de Taakgroep Cyber Security een aantal algemene uitgangspunten opgesteld voor de inventarisatie, te weten:

- De inventarisatie richt zich op alle bestaande laadinfrastructuur in Nederland die digitaal verbonden is.
- Laadstations die geen enkele communicatieverbinding hebben en enkel een stroompunt bieden, maken geen onderdeel uit van de inventarisatie.
- Het gaat om zowel reguliere laadstations (AC – vanaf 3,7 kW) als snellaadstations (DC – vanaf 50 kW) binnen het privaat, semi-publiek en publiek toegankelijke domein.
- De inventarisatie betreft uitsluitend de digitale beveiliging.

Deze uitgangspunten bieden de basis voor de verdere uitwerking van de methode en het toetskader.

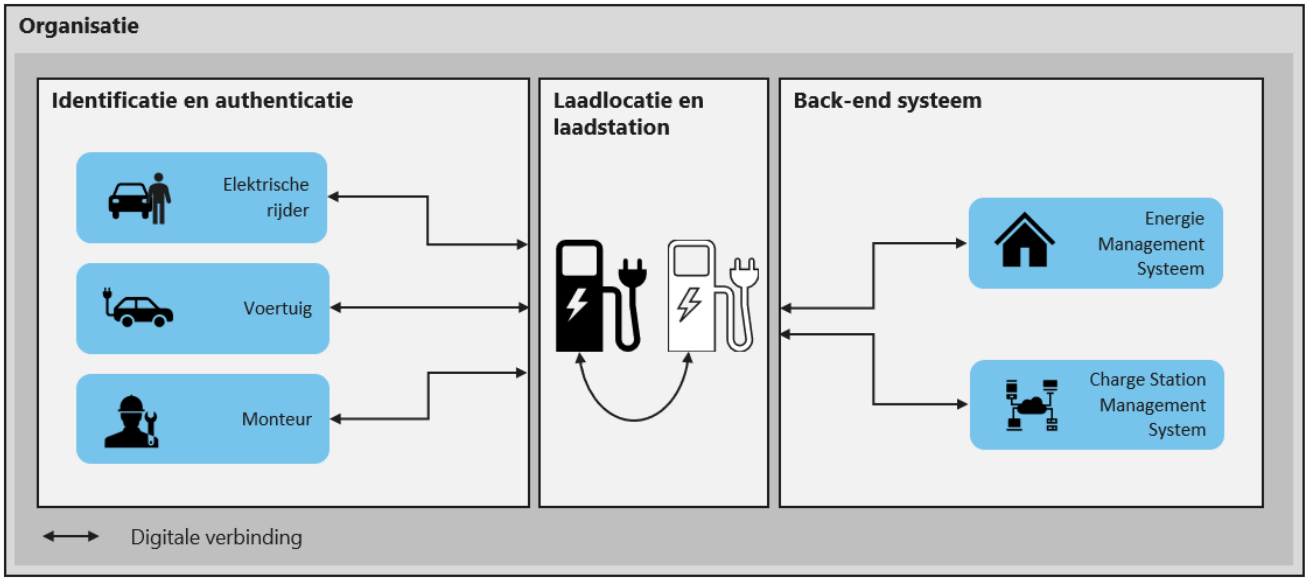
2.2 Methode

Om een zo volledig mogelijk beeld te krijgen van de stand van zaken is ervoor gekozen om informatie op te halen bij een breed aantal stakeholders die actief zijn binnen de Nederlandse markt van elektrisch vervoer en laadinfrastructuur en die werken met cybersecurity. Hierbij is een onderscheid gemaakt tussen CPO's, laadpaalleveranciers en publieke opdrachtgevers van laadinfrastructuur via aanbestedingen. Omdat de focus van de inventarisatie ligt op het laadstation en de digitale verbinding met het laadstation, zijn e-Mobility Service Providers (eMSP's) buiten beschouwing gelaten. De digitale verbinding tussen een eMSP en het laadstation verloopt namelijk via de CPO.

De informatie voor de inventarisatie is opgehaald aan de hand van een online survey en verdiepende interviews. De survey is beknopt opgesteld om de tijdsinspanning van partijen te minimaliseren en richtte zich op het verkrijgen van algemeen inzicht in onder andere gevoerd beleid en eisen, gebruikte digitale beveiliging en de wijze van digitale communicatie. Met een selectie van partijen is vervolgens een verdiepend interview gehouden waarin doorgevraagd is naar achterliggende overwegingen, keuzes en drijfveren. Deze informatie, aangevuld met de kennis van experts op het gebied van cybersecurity en experts op het gebied van laadinfrastructuur, vormt tezamen de basis van deze eindrapportage.

2.3 Toetskader

In aanvulling op de algemene uitgangspunten is een toetskader opgesteld waarin alle onderdelen en onderlinge verbindingen zijn beschreven die worden meegenomen in de inventarisatie. Het toetskader biedt daarmee een duidelijke afbakening en vormt de basis voor de survey en verdiepende interviews waarmee de informatie is verzameld. Figuur 1 geeft een overzicht van het toetskader.



Figuur 1: Toetskader inventarisatie cybersecurity laadinfrastructuur

In de snel groeiende markt van laadinfrastructuur is cybersecurity een steeds belangrijker thema, maar is dit vaak nog onderbelicht. Binnen het onderdeel **organisatie** geeft de inventarisatie inzicht in de bekendheid die marktpartijen en publieke opdrachtgevers hebben op het gebied van cybersecurity en hoe dit is belegd in de organisatie. Dit betreft onder andere of er een intern beveiligingsbeleid is waar de laadstations onderdeel van uitmaken en of er procedures zijn ingericht voor het toetsen en testen van de beveiliging, bijvoorbeeld via een externe audit.

Onder **identificatie en authenticatie** wordt het verkrijgen van digitale toegang tot het laadstation verstaan. Hierbij wordt onderscheid gemaakt tussen de elektrische rijder, het voertuig en de monteur. De EV-rijder kan op verschillende manieren toegang worden verschaft tot het laadstation, bijvoorbeeld door een laadpas langs een gebruikersinterface op de laadpaal te halen of via een mobiele applicatie van de CPO of eMSP. Er zijn echter ook mogelijkheden in ontwikkeling om identificatie via de communicatieverbinding tot stand te brengen tussen een EV en het laadstation, bijvoorbeeld via het protocol ISO 15118. Daarnaast wordt binnen de inventarisatie ook gekeken naar de lokale communicatie in het laadstation, zowel tussen componenten als menselijke interventie. Dit laatste betreft iedereen die geoorloofd digitale toegang heeft tot de binnenkant van het laadstation om technische redenen, zoals een monteur of installateur.

De **laadlocatie en laadstation** en de inkomende en uitgaande digitale verbindingen vormen het focuspunt van de inventarisatie. Onder een laadlocatie verstaan we een terrein met één adres of GPS-locatie en één CPO. Dit kan een enkel laadstation zijn, maar het kan ook over meerdere laadstations gaan die onderling verbonden zijn (bv. een laadplein). Dit systeemonderdeel kijkt onder andere naar de implementatie van beveiligingseisen, zoals van ElaadNL en ENCS[2], het doorvoeren van firmware-updates en de lokale opslag van gevoelige gegevens in het laadstation. Laadstations met een geautomatiseerde connectie, zoals een pantograaf en inductieladen, vallen buiten de scope van het toetskader.

Tot slot is in de inventarisatie gekeken naar de verbindingen van het laadstation en de laadlocatie met het **back-end systeem**. Hierbij is onderscheid gemaakt tussen de verbinding met een Energie Management Systeem (EMS) en de verbinding met het Charge Station Management System (CSMS) van een CPO. Dit onderdeel van het toetskader richt zich op welke communicatieverbindingen gebruikt worden, zoals een bedrade netwerkverbinding of WiFi, en hoe deze verbindingen beveiligd zijn middels bijvoorbeeld een protocol.

[2] Voor meer informatie over deze eisen, zie https://www.elaad.nl/projects/cybersecurity/.

3. Resultaten

De in dit hoofdstuk gepresenteerde bevindingen zijn gebaseerd op de respons op de online survey en de verdiepende interviews. Allereerst worden een aantal algemene bevindingen toegelicht. De paragrafen gaan achtereenvolgens in op de onderdelen van het toetskader, te weten de organisatie, identificatie en authenticatie, laadlocatie en laadstation en back-end systeem.

3.1 Algemene bevindingen

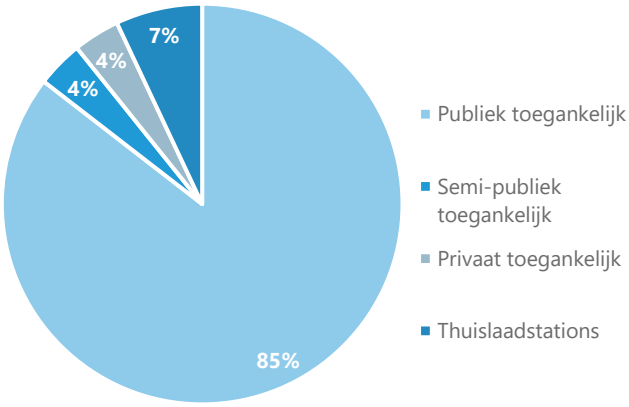
Op de online survey hebben dertien organisaties gereageerd, waarvan vier CPO's, vier laadpaalleveranciers en vijf publieke opdrachtgevers. Gezien het aantal partijen aan wie de online survey is verstuurd, was de verwachting dat de respons hoger zou liggen. Een mogelijke reden hiervoor die wij hebben gehoord van partijen is het grote aantal verzoeken om informatie te delen vanuit meerdere thema's binnen de Nationale Agenda Laadinfrastructuur, wat vraagt om het maken van keuzes.

Naast de survey zijn tien organisaties geïnterviewd. Deze gesprekken overlappen voor een deel met de respondenten van de online survey. Door de overlap en de verschillen tussen deze organisaties in omvang en aanpak geven deze respondenten samen een representatief beeld van het onderwerp. Dit is met name een kwalitatief beeld. De opgehaalde kwantitatieve informatie geeft gezien de lage respons een te nauw beeld op zichzelf. Desalniettemin is deze kwantitatieve informatie ook opgenomen in voorliggende rapportage.

Sommige marktpartijen zijn voornamelijk in Nederland actief, andere zijn internationaal actief. Marktpartijen richten zich zowel op de particuliere markt (consumenten en bedrijven), als op publiek toegankelijke laadstations. Hoewel het merendeel van de laadstations alleen AC-laden biedt, hebben ook partijen medewerking verleend die ervaring hebben met DC-snelladen met hoge vermogens van 150 kW en meer.

De respondenten van de online survey en de geïnterviewden vertegenwoordigen samen iets meer dan 120.000 laadstations waarvan ongeveer 500 snellaadstations. Hierbij moet de kanttekening geplaatst worden dat er overlap kan zitten in het aantal laadstations van de verschillende respondenten. Er kan namelijk één en hetzelfde laadstation worden bedoeld indien een publieke opdrachtgever een concessie heeft gegund aan een CPO welke de laadstations heeft ingekocht bij een leverancier, en deze partijen allemaal de survey hebben ingevuld. Daarnaast heeft een partij zich onthouden van het delen van gegevens over het areaal, gezien de bedrijfsgevoeligheid hiervan.

Aan de CPO's en publieke opdrachtgevers is aanvullend gevraagd aan te geven of de laadstations (semi)publiek of privaat toegankelijk zijn. Leveranciers zijn niet bevraagd, aangezien voor hen niet altijd bekend is waar de laadstations geïnstalleerd worden en hoe de toegang geregeld is. Het overgrote deel van het areaal van CPO's en publieke opdrachtgevers dat onderdeel uitmaakt van de survey betreft publiek toegankelijke laadstations (85%). Deze vertegenwoordigen ongeveer 70% van het totale aantal publiek toegankelijke laadstations in Nederland[3]. Het aantal privaat toegankelijke (4%) en thuislaadstations (7%) vormen een sterke ondervertegenwoordiging in de survey, gegeven dat er circa 167.000 private laadpunten in



Figuur 2: Toegang van de laadstations die onderdeel uitmaken van de survey (n=9)

[3] Gebaseerd op RVO (maart 2021), *Electric Vehicles Statistics in the Netherlands* en dat publiek toegankelijke laadstations doorgaans twee laadpunten hebben.

Nederland zijn. Het is mogelijk dat de deelnemende leveranciers aan de survey en interviews, die niet zijn bevraagd over de toegang van de laadstations, een deel van deze private en thuislaadstations vertegenwoordigen.

Gezien de gevoeligheid van het onderwerp en om anonimiteit te borgen zijn de resultaten niet herleidbaar naar individuele personen of organisaties. Dit betekent dat sommige onderzoeksresultaten wat algemener zijn geformuleerd.

3.2 Organisatie

Beveiligingsbeleid

Acht respondenten (62%) geven aan een beveiligingsbeleid te hebben dat alle laadstations betreft. Eén respondent geeft aan dat dit beveiligingsbeleid in de basis alle laadstations betreft, maar dat dit niet altijd gegarandeerd kan worden met het voortschrijden van de tijd. Er is één organisatie die aangeeft geen beveiligingsbeleid te hebben. Van de organisaties die een beveiligingsbeleid hebben heeft een enkele organisatie dit periodiek (10%) of eenmalig (30%) laten toetsen. Wanneer gevraagd of het beveiligingsbeleid ook getest wordt, geven tien van de dertien partijen aan dit periodiek (4 keer) te doen of eenmalig (6 keer) te hebben gedaan.

Op basis van de survey zou bij de meeste organisaties het beveiligingsbeleid ook de cybersecurity van de laadstations raken. Bij doorvragen in de interviews blijkt dit vaak maar beperkt of niet het geval. De beveiliging van de laadstations vloeit vaak niet direct voort uit het beveiligingsbeleid van de betreffende organisatie. De back-end systemen waarmee de laadstations worden aangestuurd kunnen wel onder het beveiligingsbeleid van de organisatie vallen. De CISO (Chief Information Security Officer) die bij de organisatie verantwoordelijk is voor cybersecurity heeft bij de meeste organisaties geen actieve rol bij de beveiliging van de laadstations. Bij sommige organisaties die hebben meegewerkt aan dit onderzoek is deze rol wel nadrukkelijk belegd bij de CISO en een enkele organisatie heeft zelfs een afzonderlijke functionaris voor de beveiliging van de laadstations.

Uit bovenstaande resultaten blijkt dat er niet bij alle organisaties een beveiligingsbeleid is. Omdat cybersecurity een plek in de organisatie nodig heeft om de juiste aandacht te krijgen, vormt dit een potentieel risico. De organisaties die meewerkten aan de interviews schetsen wel een beeld hoe cybersecurity een plek heeft in hun organisatie. Bij de leveranciers zijn er bijvoorbeeld mensen in de organisatie belast met de specifieke taak om beveiligingsrichtlijnen op te stellen en bij te stellen, die vervolgens worden verwerkt in de systeemarchitectuur (hardware en firmware) van het laadstation. Het testen van de beveiliging is een vast onderdeel bij iedere (door)ontwikkeling van het laadstation, blijkt uit de gesprekken met de diverse leveranciers.

CPO's onderwerpen de laadstations aan een test voordat deze worden afgenomen, waarbij ook de beveiliging wordt getest. Bij de marktpartijen is dit sterker dan bij de publieke opdrachtgevers, maar ook bij deze opdrachtgevers komt hier steeds meer aandacht voor. Dat wordt bijvoorbeeld zichtbaar bij deze organisaties in richtlijnen voor de beveiliging die in de meest recente concessies werden meegenomen. Zowel mensen die betrokken waren bij de beveiligingseisen in de aanbesteding, maar ook mensen vanuit de afdeling inkoop namen deel aan de interviews. In de gesprekken werd duidelijk dat cybersecurity vooral voor de meest recente concessieverleningen een rol speelt en met name bij de grotere opdrachtgevers in de publieke sector die betrokken waren bij voorliggende inventarisatie.

Verantwoordelijkheden

Uit de interviews blijkt dat publieke opdrachtgevers er in het verleden op vertrouwden dat CPO's zouden zorgen dat aan beveiligingseisen zou worden voldaan. CPO's vertrouwden er op hun beurt op dat hun opdrachtnemers, de leveranciers van laadstations, daarvoor zouden zorgen. Zo is een vorm ontstaan van gedelegeerde verantwoordelijkheid die tot op de dag van vandaag voortduurt. Deze verantwoordelijkheid is met name gebaseerd op vertrouwen en minder op expliciete afspraken. Hoewel uit de interviews geen

veiligheidsincidenten naar voren komen, geven partijen aan zich er bewust van te zijn dat cybersecurity aandacht behoeft om te voorkomen dat zulke incidenten zich op enig moment in de tijd voor zullen doen. De voorbeelden van mogelijke risico's die genoemd werden, zoals het gelijktijdig verstoren van grote aantallen laadsessies, illustreren dat de risico's groter worden met de groei van de laadinfrastructuur.

Met de toenemende aandacht voor cybersecurity wordt er actiever invulling gegeven aan de verantwoordelijkheid als opdrachtgever. Publieke opdrachtgevers die zijn geconsulteerd voelen zich juridisch verantwoordelijk, met als resultaat dat zij tegenwoordig actief eisen stellen aan de beveiliging bij de verlening van een concessie. CPO's vertalen deze beveiligingseisen vervolgens naar eisen die zij aan de laadpaalleveranciers stellen. Omdat inhoudelijke kennis over hoe en wat er beveiligd moet worden onvoldoende aanwezig is bij de publieke opdrachtgevers, maken zij gebruik van de kennis die hierover bij ElaadNL en ENCS is opgedaan. ElaadNL en ENCS hebben op basis van die kennis een richtlijn[4] ontwikkeld, die in toenemende mate door publieke opdrachtgevers als onderdeel van het programma van eisen aan de concessie wordt toegevoegd.

Richtlijn van ElaadNL en ENCS

In het verleden formuleerden marktpartijen die beveiligingseisen zelf; publieke opdrachtgevers beschikten destijds niet over een norm waaraan moest worden voldaan. Omdat de behoefte aan een richtlijn breed werd gevoeld hebben ElaadNL en ENCS bovenvermelde beveiligingsrichtlijn ontwikkeld voor laadinfrastructuur. Marktpartijen die medewerking hebben verleend aan de interviews zijn echter van mening dat de richtlijn teveel nadruk legt op de risico's voor de netbeheerder, terwijl voor hen niet duidelijk is of dat risico dusdanig groot is. Daarnaast vinden marktpartijen dat de richtlijn soms te gedetailleerd voorschrijft hoe iets moet worden opgelost, in plaats van dat het moet worden opgelost. Zij geven aan dat er bijvoorbeeld technieken voor de beveiliging worden voorgeschreven, zoals de wijze waarop fysieke toegang tot het laadstation gedetecteerd moet worden, terwijl marktpartijen behoefte hebben aan functionele voorschriften zodat zij daar zelf de juiste techniek bij kunnen kiezen. Zij geven aan dat dit ruimte biedt voor nieuwe en innovatieve technieken. In 2019 zijn aangepaste richtlijnen van ElaadNL en ENCS verschenen die hier (deels) aan tegemoet komen. In dit onderzoek is dit onderscheid en hoe dat door marktpartijen is ontvangen niet verder uitgewerkt.

Testen van de beveiligingseisen van het laadstation

Marktpartijen zijn gewend te testen of hun eigen laadstations aan de beveiligingseisen voldoen. Uit de survey en verdiepende interviews blijkt dat testen in beginsel eenmaal worden uitgevoerd. De leverancier test bij iedere ontwikkeling of een laadstation voldoet aan alle eisen die volgen uit hun eigen richtlijn en de eisen die worden gesteld door hun opdrachtgever. De CPO's die we hebben gesproken testen voordat de laadstations worden afgenomen en hanteren hierbij eigen beveiligingsrichtlijnen aangevuld met beveiligingseisen van een opdrachtgever. Eén van de betrokken CPO's laat bovendien periodiek de beveiliging opnieuw testen.

Niet alle publieke opdrachtgevers testen de laadstations. Slechts drie van de vijf respondenten hebben de beveiliging eenmalig laten testen bij het verlenen van de concessie. Nu publieke opdrachtgevers in de recentere concessies ook aandacht besteden aan de beveiligingseisen, beseffen zij dat zij bij wijze van controle ook deze cybersecurity-eisen van de laadstations moeten (laten) testen. Dit is gebleken uit de gesprekken die we hebben gevoerd. De kennis over de beveiliging en het bewustzijn dat hier op getest moet worden stond niet bij iedere opdrachtgever voldoende op het netvlies. Daarom worden door enkele opdrachtgevers met terugwerkende kracht alsnog eisen ingevoerd bij de reeds geplaatste laadstations waarvan bij de concessiehouder is geëist dat ze aan de beveiligingseisen moeten voldoen. Voor overige laadstations uit oudere concessies zullen nog afspraken moeten worden gemaakt over de beveiligingseisen. Het ontmantelen, updaten of vervangen van deze laadstations hangt af van levensduur van het laadstation en contractduur. Het is hierdoor moeilijk om algemene uitspraken te doen over deze laadstations.

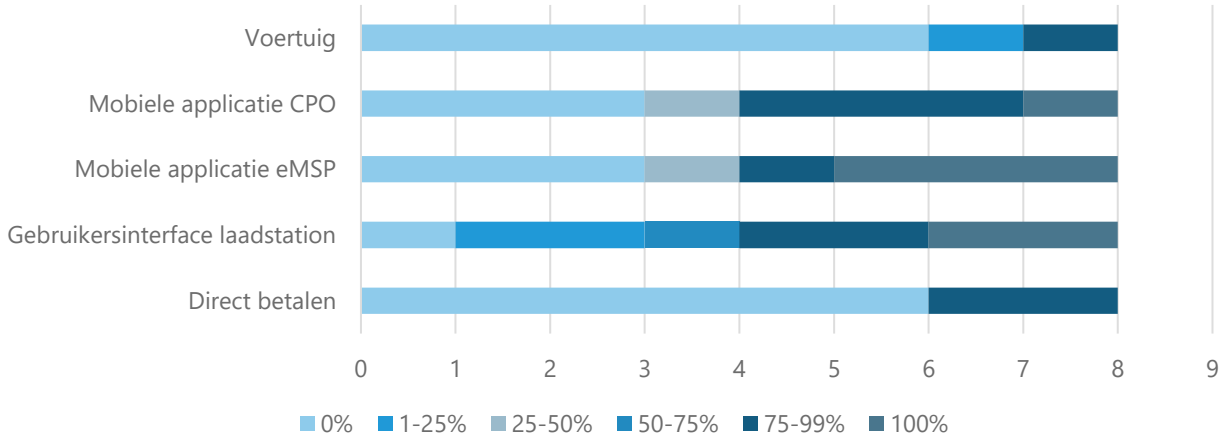
[4] Zie *Security requirements for procuring EV charging stations*: https://encs.eu/encs-document/security-requirements-for-procuring-ev-charging-stations/

3.3 Identificatie en authenticatie

Mogelijkheden tot autorisatie laadsessies

Voordat een EV kan starten met laden bij een laadstation dient de EV-rijder geïdentificeerd en geautoriseerd te worden. Er bestaan verschillende mogelijkheden om laadsessies te autoriseren, te weten:

1. *Direct betalen*: Bij het laadstation zelf betalen via een betaalterminal met bv. bankpas of creditcard. Dit gebeurt in principe altijd met betaalterminals die door de financiële wereld zijn getest en geautoriseerd (vergelijkbaar met pinautomaten bij winkels).
2. *Gebruikersinterface laadstation*: De EV-rijder authentiseert zichzelf op het laadstation, bv. met een token of laadpas. Hiervoor worden RFID-kaarten gebruikt zonder aanvullende beveiligingsmaatregelen (zoals bv. een pincode).
3. *Mobiele applicatie eMSP*: De EV-rijder identificeert zichzelf via een app van zijn eMSP op zijn smartphone. Door aan te geven bij welk laadstation de EV geladen moet worden, kan de laadsessie worden geautoriseerd.
4. *Mobiele applicatie CPO*: Hierbij gebeurt het op dezelfde manier als via de mobiele applicatie van de eMSP, maar neemt de CPO de autorisatie voor zijn rekening.
5. *Voertuig*: De EV-rijder sluit alleen de laadkabel aan en het laadstation herkent het voertuig. Op basis hiervan kan het laadstation de laadsessie direct starten ('plug & charge').



Figuur 3: Bij hoeveel laadstations vindt autorisatie plaats via direct betalen, gebruikersinterface, etc.? (n=8)

Laadstations kunnen meerdere identificatiemogelijkheden bieden, waardoor het totale percentage hoger ligt dan 100%. Uit de survey blijkt dat autorisatie van de laadsessie via direct betalen mogelijk is voor een klein deel van de laadstations. Twee partijen bieden dit aan. Daarnaast zijn autorisatie via een mobiele applicatie van de CPO of eMSP het meest voorkomend (beide 63%). In de meeste gevallen dient de EV-rijder vervolgens aan te geven op welk laadstation hij de laadsessie wil starten. Partijen geven aan dat dit vaak gebeurt middels een te scannen QR-code. Op het merendeel van de laadstations van de respondenten (88%) gaat autorisatie via een gebruikersinterface waar een laadpas met RFID-chip kan worden gelezen. In Nederland zijn de laadpassen met RFID uitgegroeid tot de standaard en zijn dat tot heden nog steeds. Sinds kwetsbaarheden van de huidige laadpassen aan het licht kwamen (mede door het onderzoek naar de ov-chipkaart die een vergelijkbare Mifare-chip gebruikte) twijfelen sommige geïnterviewde organisaties of de beveiliging beter moet. De beveiliging van de laadpassen kan indien gewenst verbeterd worden met bijvoorbeeld een pincode. Niet alle organisaties vinden de kosten van een dergelijke upgrade opwegen tegen het risico van de huidige pas.

Autorisatie via voertuig

Partijen geven aan dat het voertuig momenteel nauwelijks als authenticatie wordt gebruikt. Twee partijen geven aan dat hun laadstations op dit moment deels geschikt zijn voor directe communicatie met het voertuig. ISO 15118 is recent als standaard hiervoor ontwikkeld en slechts bij enkele nieuwe automodellen geïmplementeerd. In de survey zijn CPO's en leveranciers gevraagd of laadstations geschikt zijn voor de specifieke toepassing van deze standaard. Vijf van de acht partijen geven aan dat een deel, variërend van 1 tot 75%, van hun laadstations hiervoor voorbereid zijn. De overige drie partijen geven aan dat geen enkel laadstation voorbereid is. Uit de interviews blijkt wel dat veel partijen erkennen dat deze oplossing toekomst heeft.

Aanvullend blijkt uit de gesprekken dat deze ISO-standaard vragen oproept rond de marktordening. Verschillende partijen (OEM, CPO, eMSP) hebben er baat bij om de klant, de EV-rijder, aan zich te binden. Als de laadsessies door het voertuig kunnen worden geautoriseerd in plaats van een laadpas, is de vraag welke rol er voor de eMSP en welke voor de OEM is bij deze autorisatie. Omdat het protocol ook beschrijft hoe de laadsnelheid of zelfs het terug laden van stroom wordt gestuurd, zijn er ook discussies over de rol van netbeheerder, CPO en OEM met de komst van dit protocol. De ISO-standaard biedt dus niet alleen een extra mogelijkheid voor de autorisatie van laadsessies. Dit vraagt fundamentele keuzes en regie op internationaal niveau. Daarom, en vanwege de beperkte beschikbaarheid van laadstations en voertuigen die momenteel geschikt zijn voor ISO 15118, is het de vraag of ISO 15118 al binnenkort op grote schaal zal worden toegepast.

Autorisatie monteur

Er zijn diverse manieren waarop de lokale toegang tot de controller en de firmware in het laadstation toegankelijk wordt gemaakt voor monteurs. Een groot deel van de laadstations van de respondenten hebben een vorm van fysieke beveiliging. Twee van de acht partijen geven aan geen fysieke toegangsdetectie te hebben op de laadstations. Waar bij het ene laadstation een monteur aan eisen moet voldoen voor er een fysieke sleutel voor het cilinderslot wordt uitgegeven, is voor het andere laadstation een laptop met certificaat nodig om toegang te krijgen tot de controller. Experts geven aan dat multifactor-authenticatie (MFA) een waardevolle aanvulling kan zijn om deze beveiliging te verbeteren, als daar naar aanleiding van een risico-inventarisatie behoefte aan mocht zijn. Een monteur zou dan ook een toegangscode moeten opvragen voor digitale toegang. MFA lijkt momenteel geen standaard onderdeel van deze beveiliging en de aanpassing van systemen en werkprocessen die hiervoor nodig zijn brengen kosten met zich mee.

De fysieke toegang wordt niet bij alle laadstations gedetecteerd of gelogd. De meningen over het nut hiervan verschillen in grote mate tussen de geïnterviewden. De meeste organisaties zien het niet als strikt noodzakelijk voor de digitale beveiliging bij alle laadstations, omdat ook bij fysieke toegang tot het laadstation er nog geen digitale toegang tot de lokale computer in het laadstation is. Overigens registreren alle partijen die we hier over hebben gesproken de toegang tot de lokale controller van het laadstation. Als de fysieke toegang niet gedetecteerd wordt dan gebeurt dit wel voor het inloggen (of pogingen daartoe).

3.4 Laadlocatie en laadstation

Firmware-updates

Firmware is de software die draait op de hardware van het laadstation en die nodig is om de verschillende functies in het laadstation aan te sturen. Firmware die nu veilig wordt geacht is dat mogelijk op enig toekomstig moment niet meer. Daarvoor zullen firmware-updates met enige regelmaat moeten worden uitgebracht en geïmplementeerd. De frequentie waarmee deze updates beschikbaar worden gesteld zijn geen directe indicatie voor de mate van beveiliging. Er zijn voorbeelden bekend van updates die de beveiliging verslechterden. Wanneer er lange tijd tussen de updates zit kunnen potentiële beveiligingslekken echter langer voortduren, De aangepaste of nieuwe firmware wordt geleverd door de leverancier van het laadstation. Partijen geven in de

survey aan dat de primaire verantwoordelijkheid voor de uitrol van deze firmware bij de CPO ligt (75%). Eén partij geeft aan dat de leverancier de updates doorvoert en een andere partij geeft aan dat naast de CPO ook andere derde partijen geautoriseerd zijn voor toegang.

In het geval dat de leverancier de updates doorvoert, hebben zij toegang nodig tot de laadstations, waarmee de CPO's moeten instemmen. Zo kunnen leveranciers direct de update uitrollen op de betreffende laadstations en zijn zij niet afhankelijk van de CPO. Daar waar de firmware-update van het laadstation invloed heeft op de verbinding met het Charge Station Management Systeem (CSMS) kan soms ook een update van dit CSMS nodig zijn. Dit wordt nader toegelicht in paragraaf 3.5 Back-end systeem. Omdat veel laadstations met een SaaS-oplossing worden beheerd zijn deze CSMS-updates eenvoudiger door te voeren. Aanbieders van een SaaS-oplossing bedienen meerdere organisaties met hun software. Zij kunnen zo met één update meerdere organisaties voorzien van de nieuwe verbeterde oplossing.

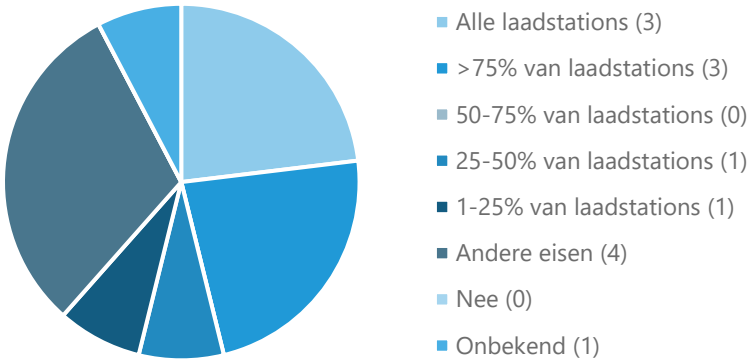
De frequentie van de firmware-updates is heel wisselend, variërend van ad hoc (38%) tot maandelijks (13%) of enkele keren per jaar (38%). Eén partij geeft aan dat onbekend is met welke frequentie updates worden doorgevoerd. Voor zover bekend uit de interviews hebben alle leveranciers het besef dat updates niet kunnen wachten bij belangrijke kwetsbaarheden in de firmware. Afspraken over het updateproces van de firmware zijn een onderdeel van de richtlijn van ElaadNL en ENCS. Of er voor de laadstations die niet onder deze richtlijn vallen ook afspraken zijn gemaakt tussen opdrachtgevers en leveranciers blijkt niet uit het onderzoek. Er is geen garantie dat updates blijven komen na afloop van het contract als de economische levensduur van het laadstation nog niet voorbij is. In de huidige praktijk blijkt dit op basis van de gevoerde gesprekken (nog) niet tot problemen te leiden. De leveranciers die hierover zijn bevraagd blijven hun best doen om kwetsbaarheden op te lossen en stellen de firmware beschikbaar voor laadstations als dat mogelijk is, ook na het einde van een eventuele contractdatum.

Soms vormt de hardware een belemmering voor de firmware-updates. Betere beveiliging, bijvoorbeeld voor versleuteling van gegevens, vraagt soms ook zwaardere hardware (bv. groter geheugen of meer rekencapaciteit). Hardware vervangen is kostbaar en is niet altijd kosteneffectief, omdat hiervoor een monteur het laadstation moet bezoeken. Dit geldt met name voor de oudere laadstations waarvoor de hardware vaak ontoereikend is. Bij nieuwe laadstations en met name bij laadstations met hoge laadvermogens is de hardware vaak ook zwaarder uitgevoerd. Dit geldt al voor de laadstations vanaf 50 kW en zeker voor de laadstations van 350 kW voor ultrasnelladen. In deze gevallen is de hardware vaak minder een belemmering voor de digitale beveiliging.

Updates kunnen in bijna alle gevallen (88%) op afstand worden doorgevoerd. Een enkele partij geeft aan dat dit op afstand kan, maar niet voor alle componenten (12%). In bijzondere gevallen is een monteur ter plekke nodig. Dit maakt een snelle uitrol van updates lastiger en bovendien kostbaarder. Het is ook afhankelijk van de toegankelijkheid van het netwerk waar het laadstation mee is verbonden. Als dit een gesloten netwerk is, is eerst toegang tot dit gesloten netwerk nodig (zie ook paragraaf 3.5 Back-end systeem).

Implementatie beveiligingsrichtlijn van ElaadNL en ENCS

Slechts drie partijen geven aan de cybersecurity requirements van ElaadNL en ENCS te hebben geïmplementeerd op alle laadstations. Drie andere partijen hebben de richtlijn op meer dan 75% van hun totale areaal geïmplementeerd.



Figuur 4: Zijn de cybersecurityeisen van ElaadNL en ENCS geïmplementeerd bij de laadstations? (n=13)

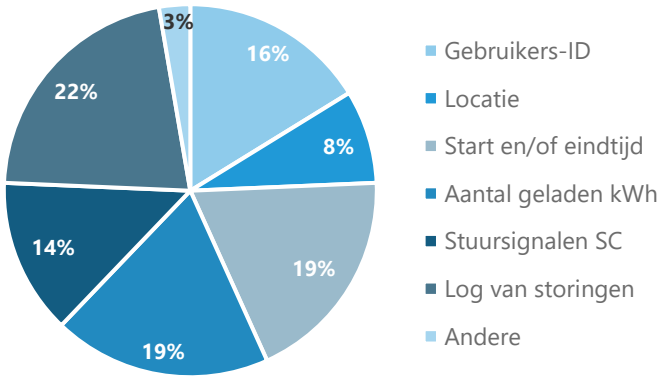
Door vier respondenten wordt aangegeven dat andere eisen zijn geïmplementeerd. De redenen hiervoor lopen uiteen. Eén partij is niet bekend met de eisen van ElaadNL en ENCS en daarnaast wordt aangegeven dat de implementatie afhankelijk is van het type laadpalen (publiek of privaat toegankelijk) en het type verbinding (met een sim of via internet). Eén van deze respondenten geeft in een interview aan zelf met experts beveiligingseisen te hebben opgesteld en ook eisen te implementeren die door andere opdrachtgevers worden gevraagd. Publieke opdrachtgevers is aanvullend gevraagd of de eisen met terugwerkende kracht zijn geïmplementeerd op oudere laadstations. Dit blijkt bij de helft van de publieke opdrachtgevers gebeurd te zijn, waarbij één opdrachtgever aangeeft dit voor alle laadstations te hebben gedaan.

Partijen geven in de interviews aan de richtlijn niet als onoverkomelijk te beschouwen, alhoewel enkele marktpartijen vraagtekens stellen bij de onderbouwing van beveiligingseisen. Ze hebben behoefte aan een goed beeld van de kans en de impact van de beveiligingsrisico's die hier aan ten grondslag liggen. Omdat de richtlijn van ElaadNL en ENCS nog relatief jong is, is deze bij publieke opdrachtgevers die de online survey hebben ingevuld pas bij de meest recente concessies geïmplementeerd bij laadstations vanaf 2019 of 2020. Er zijn daarom maar weinig laadstations te vinden die aan deze eisen voldoen. Sommige leveranciers en CPO's hebben nog niet met deze eisen te maken gehad.

De ervaring leert dat niet altijd alle partijen in één keer aan deze eisen voldoen. Dit is voor een belangrijk deel onbekendheid met de exacte implicaties van deze beveiligingsrichtlijn. Voor de publieke opdrachtgevers die wij hebben gesproken is dit aanleiding om de beveiliging onafhankelijk te laten toetsen. Bij laadstations waar de richtlijn niet is geïmplementeerd gebeurt dat enkel met terugwerkende kracht als het laadstation daar geschikt voor is. Een van de publieke opdrachtgevers gaf aan hiervoor met een derde onafhankelijke organisatie te werken die kennis heeft van de laadinfrastructuur. Zo kan alsnog worden vastgesteld of de laadstations voldoen aan de beveiligingseisen die bij de concessie zijn gesteld. Aan de hand hiervan worden voor de betreffende concessie de beveiligingseisen alsnog geïmplementeerd bij de laadstations die er nog niet aan voldeden.

Lokale gegevensopslag

Er worden diverse gegevens lokaal opgeslagen in het laadstation, met name start- en/of eindtijd (19%), aantal geladen kWh (19%) en een log van storingen of foutmeldingen (22%). Dit zijn geen bijzonder gevoelige gegevens en gegevensbeveiliging is hiervoor niet direct van groot belang. In sommige gevallen worden gegevens opgeslagen in het laadstation die herleidbaar zijn tot personen, vaak in combinatie met andere bestanden zoals een laadpas-id. Hiervoor is beveiliging nodig. Het beeld dat het daarmee meteen persoonsgegevens zijn, wordt niet



Figuur 5: Welke van de volgende gegevens worden lokaal opgeslagen in het laadstation? (n=8)

door iedere organisatie zo gezien[5]. Desondanks hebben alle partijen die wij hierover spraken maatregelen genomen om de gegevens af te schermen. Om bij de gegevens te komen heb je fysiek toegang nodig tot de binnenkant van het laadstation en dan is er vaak digitale beveiliging, bijvoorbeeld via versleuteling of gecertificeerde apparatuur, die de gegevens beschermen.

Eichrecht

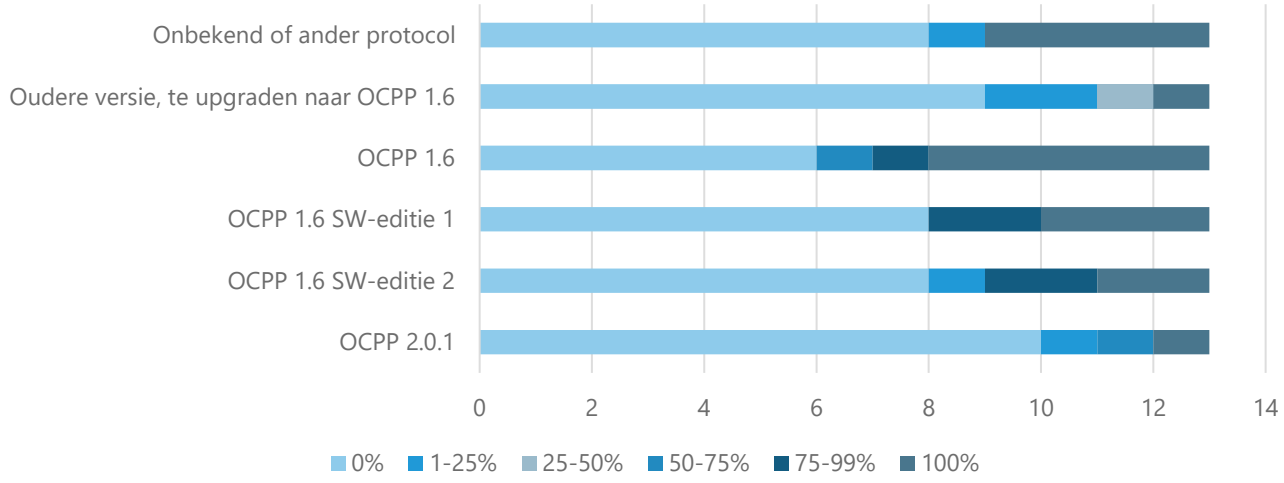
In Duitsland zijn er uitgebreide richtlijnen die voorschrijven hoe de geijkte meterstanden per laadsessie zorgvuldig vanuit de meter (zowel AC als DC) bij de EV-rijder te krijgen[6]. Hiervoor is digitale beveiliging van deze gegevens nodig (bv. digitale certificaten, versleuteling) die bewaken dat deze meterstanden niet gemanipuleerd worden in het laadstation of elders in de keten. Tot voor kort waren er voor DC-laadstations nog geen goede geijkte meters beschikbaar. Nu deze zijn ontwikkeld, is er geen belemmering meer om deze in te zetten.

Marktpartijen zijn zich er van bewust dat deze ontwikkeling niet voorbehouden blijft tot de Duitse markt. Sommige van de geïnterviewde marktpartijen roepen zelfs op om deze 1-op-1 over te nemen voor de Nederlandse markt, al is hier nog discussie over. Als deze regelingen uit het Duitse Eichrecht, al dan niet aangepast, ook in Nederland worden ingevoerd dan is er voor de bestaande laadinfrastructuur een inhaalslag nodig die tijd nodig heeft.

3.5 Back-end systeem

Verbinding laadstation en back-end

OCPP is een protocol dat de communicatie beschrijft van de verbinding tussen het laadstation en de back-end. Dit protocol is voor de publiek toegankelijke laadinfrastructuur in Nederland het meest gebruikt. Vanaf OCPP 1.6 SW-editie 1 is basale digitale beveiliging onderdeel van dit protocol.



Figuur 6: Geef per versie van OCPP aan hoeveel laadstations hiermee zijn uitgerust (n=13)

De laadstations van zeven van de respondenten (54%) zijn volledig of deels uitgerust met OCPP 1.6. De recentere versies OCPP 1.6 SW-editie 1 en 2 komen ook terug in de survey. Uit de verdiepende interviews blijkt dat er weinig laadstations zijn met oudere versies dan het protocol OCPP 1.6. Meestal gaat het om oude laadstations die niet eenvoudig geüpdatet kunnen worden omdat de hardware daarvoor niet toereikend is. Omdat dit oude laadstations zijn die het einde van hun technische en economische levensduur naderen, wordt

[5] Zie ook paragraaf 3.2 Handleiding Autoriteit Persoonsgegevens

[6] Onderzoek over het Eichrecht German charging infrastructure regulations (rvo.nl)

dit niet direct als een probleem gezien door organisaties. Zij geven aan dat dit zichzelf oplost als deze laadstations de komende jaren worden vervangen. Om te voorkomen dat er in de publieke ruimte toch een enkel laadstation zou blijven staan met een verouderd, onbeveiligd communicatieprotocol zou je een deadline moeten stellen waarop deze uiterlijk geüpdatet of vervangen moet zijn, als het risico dat zou rechtvaardigen.

In de recente OCPP-versie 2.0.1 is de beveiliging significant verbeterd. De beveiliging die deel uitmaakt van deze OCPP-versie is ook beschikbaar gemaakt voor OCPP versie 1.6 als optionele update. Zoals te zien in figuur 6 blijkt uit de survey dat deze OCPP 1.6 editie 2 bij een beperkt deel van de laadstations is geïmplementeerd en laadstations met het nieuwe OCPP 2.0.1-protocol nog minder te vinden zijn. Deze versie is door drie partijen op een deel van de laadstations (67%) of op alle laadstations (33%) geïmplementeerd. Publieke opdrachtgevers geven in de interviews aan dat in nieuwe concessies altijd deze nieuwste versie van dit protocol gevraagd wordt.

Marktpartijen beseffen dat dit niveau van beveiliging nodig is en willen laadstations die hiervoor geschikt zijn er ook mee uitrusten. Als oudere laadstations niet geschikt zijn kunnen ze worden vervangen door nieuwe laadstations, maar dit beperkt de uitrol van nieuwe laadstations waarmee zij hun areaal uitbreiden. Alle organisaties, zowel markt als overheid, zijn zich er van bewust dat ook aan die opgave gewerkt moet worden. Er is geen universele oplossing voor hoe moet worden omgegaan met deze oudere laadstations. Per keer wordt door organisaties gekeken wat technisch en economisch haalbaar is.

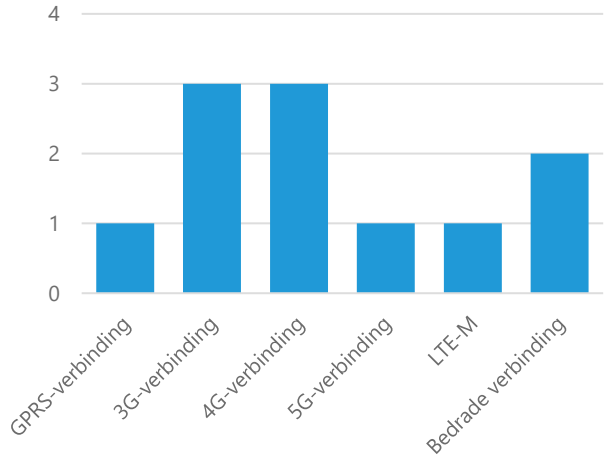
Ook het CSMS zal overweg moeten kunnen met de nieuwste versie van OCPP. Dit zal bij grote updates van het OCPP-protocol vaak een grotere inspanning vragen. Op basis van de gevoerde gesprekken lijkt dit niet onoverkomelijk, maar bij het uitbrengen van een nieuwe versie van OCPP zullen niet direct alle CSMS'en zijn voorzien van deze versie.

Communicatieverbinding

Uit de survey blijkt dat het voor de organisaties die hierop hebben gereageerd ongebruikelijk is om een bedrade communicatieverbinding te hebben tussen het CSMS en het laadstation, zoals glasvezel of koperkabel. Respondenten geven aan voornamelijk mobiele telefonieverbindingen te gebruiken. Hierbij wordt gebruik gemaakt van publieke telefonienetwerken (zie figuur 7). Uit de interviews blijkt dat enkele organisaties uit kostenoogpunt overwegen om meerdere laadstations die bij elkaar op één laadlocatie staan gebruik te laten maken van één mobiele telefonieverbinding. Die laadstations kunnen dan via een lokaal bedraad netwerk gebruik maken van eenzelfde modem voor mobiele telefonie.

Om veilig te communiceren wordt door één CPO een VPN-verbinding gebruikt. Meer gebruikelijk is beveiliging middels OCPP 1.6 (25%), OCPP 1.6 SW-editie 1 (13%), OCPP 1.6 SW-editie 2 (25%) en OCPP 2.0.1 (13%). Alle leveranciers geven daarnaast aan dat de laadstations die zij leveren versleutelde communicatiemogelijkheden middels OCPP bieden, waarbij SW-editie 1 en 2 het meeste genoemd worden.

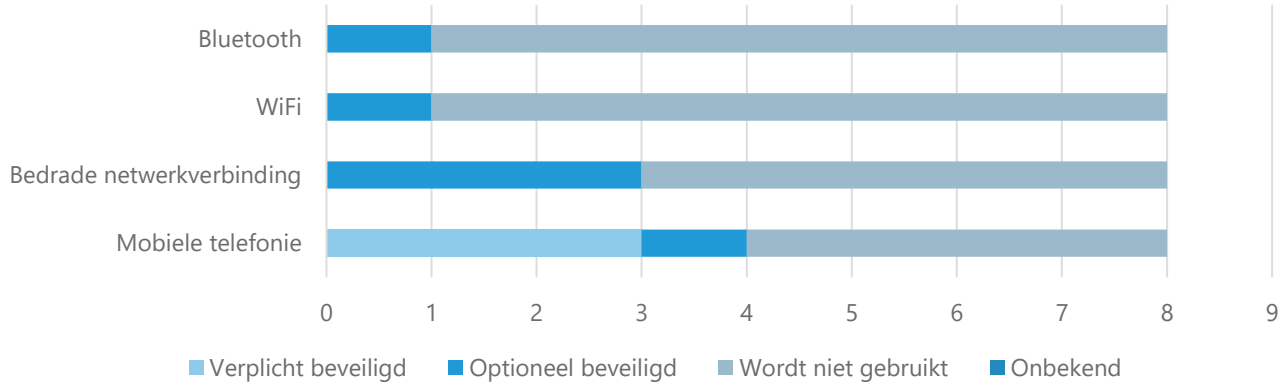
Ook bij laadlocaties met meerdere laadstations (bv. laadpleinen) zijn er voor organisaties die meewerkten aan dit onderzoek vaak geen lokale verbindingen en hebben de laadstations hun eigen afzonderlijke verbinding met het CSMS.



Figuur 7: Welke communicatieverbindingen worden toegepast tussen het CSMS en de laadlocatie? (n=4)

Respondenten van de survey geven aan dat hun laadstations meestal geen lokale dataverbinding hebben. De meeste zijn uitsluitend verbonden met een CSMS van de CPO. Daar waar laadstations wel de mogelijkheid bieden om verbinding te maken met een lokaal netwerk is het altijd mogelijk om deze te beveiligen. Een van de geïnterviewde marktpartijen ziet hierbij ook de mogelijkheid voor een stabielere en meer kosteneffectieve verbinding bij laadstations voor particulieren.

Naast een koppeling met het CSMS kan een laadstation ook verbonden worden met een energie management systeem (EMS). Op basis van de respons op de survey lijkt dit maar voor een beperkt deel van de laadstations gebruikt te worden (zie figuur 8). Als het gebruikt wordt is de verbinding tussen het laadstation en het EMS vaak wel te beveiligen. In een enkel geval wordt deze beveiliging ook afgedwongen door de firmware in het laadstation en werken onbeveiligde verbindingen niet.



Figuur 8: Welke communicatieverbindingen worden gebruikt tussen het laadstation en het EMS en zijn deze beveiligd? (n=8)

Beveiliging CSMS

Voorliggende inventarisatie richt zich op de laadstations en op de verbindingen met dit laadstation. De laadinfrastructuur als geheel bevat echter veel meer systemen die veilig moeten zijn van het energienet tot en met het voertuig. Bij het onderzoek naar de beveiliging van de laadstations kwam de rol van het CSMS naar voren. Deze beveiliging is niet expliciet onderzocht, aangezien dit buiten de scope viel. Wel werd duidelijk dat de beveiliging van de laadstations voor een belangrijk deel afhankelijk is van de beveiliging van dit CSMS. Voor de updates van de firmware, voor de autorisatie van de laadsessies en voor de aansturing van de laadsessies speelt het CSMS een cruciale rol. Dat betekent dat er ook aandacht moet zijn voor de beveiliging van deze CSMS'en (software en procedures rondom autorisatie) om de laadinfrastructuur goed te beveiligen. De impact op de laadstations kan bijzonder groot zijn als er veel laadstations worden aangestuurd met het CSMS. In het geval van SaaS-oplossingen die door meerdere CPO's worden gebruikt kunnen de aantallen aangestuurde laadstations hoog oplopen.

4. Conclusies en aanbevelingen

4.1 Conclusies

Op basis van een online survey en verdiepende interviews onder CPO's, leveranciers van laadstations en publieke opdrachtgevers is een beeld gevormd van de huidige cybersecurity van de laadinfrastructuur in Nederland. De markt voor laadinfrastructuur is nog relatief jong en er zijn veel nieuwe partijen in actief. Desondanks zijn er al veel standaarden en normen ontwikkeld, maar voor de cybersecurity is dit de laatste jaren sterk in ontwikkeling. Een groot deel van de laadstations die onderdeel uitmaken van deze inventarisatie bezitten een vorm van digitale beveiliging, zoals versleutelde verbindingen tussen het laadstation en het back-end systeem. De mate waarin loopt echter sterk uiteen, getuige onder andere het feit dat niet alle organisaties een beveiligingsbeleid hebben wat zij laten toetsen en de variërende implementatie van de cybersecurity requirements van ElaadNL en ENCS. De organisaties waarmee is gesproken erkennen dat er kwetsbaarheden zijn ten aanzien van de cybersecurity. Hoe groot deze risico's zijn, hoe groot de impact is en hoe groot de kans is dat het zich voordoet, is niet bij iedere organisatie even duidelijk.

Nederland heeft een koplopersrol op het gebied van laadinfrastructuur met de meeste laadstations van de Europese Unie. Deze rol leidt er ook toe dat er op dit moment verouderde laadstations zijn die volgens de organisaties die wij hebben gesproken niet meer geüpdatet kunnen worden met de meest recente beveiligingseisen. Dit betreft met name publiek toegankelijke laadinfrastructuur. Op basis van de beperkte respons zijn de exacte aantallen niet te bepalen. Deze minder veilige laadstations vormen een beveiligingsrisico en zullen op termijn moeten worden vervangen. De deelnemende organisaties aan dit onderzoek zien hierbij geen acuut risico. Zij geven aan dat de meeste van deze laadstations de komende jaren worden vervangen vanwege de technische en economische levensduur. In gezamenlijkheid dient te worden bepaald wanneer deze laadstations uiterlijk moeten zijn aangepast of vervangen.

4.2 Aanbevelingen

Op basis van de inventarisatie komen we tot een drietal aanbevelingen die worden gezien als belangrijke punten voor vervolgstappen bij de digitale beveiliging van de laadinfrastructuur.

Inventariseer de risico's

Een aanbeveling is om de verschillende risico's die een gebrekkige beveiliging met zich meebrengt zowel wat betreft kans als impact in beeld te brengen om het belang van de beveiligingseisen goed te kunnen wegen. Als er slechts op kleine schaal gefraudeerd kan worden met laadsessies is de autorisatie een kleiner probleem dan wanneer dit op grote schaal gebeurt. Als het hacken van laadstations grote delen van het laad- en elektriciteitsnetwerk plat kunnen leggen verdient dit meer aandacht dan wanneer alleen het betreffende laadstation tijdelijk buiten gebruik is. Als eisen duidelijk gerelateerd kunnen worden aan de risico's, is er naar verwachting minder discussie over deze eisen en vergroot dit de samenwerking tussen alle partijen om hier aan te voldoen.

Geadviseerd wordt om in de risico-inventarisatie een onderscheid te maken in type laadstation, omdat de risico's hiervoor mogelijk anders zijn. De impact op laadstations voor bussen op OV-lijnen of voor grote laadpleinen met snelladers zouden een ander risico kunnen vormen dan thuisladers. Indien thuislaadstations van hetzelfde type in grote aantallen zijn geïnstalleerd wordt ook hiervoor mogelijk het risico groter. Vanwege de cruciale rol die het CSMS speelt bij de aansturing van de laadstations en daarmee ook bij de digitale veiligheid van deze laadstations, is het goed om bij een risico-inventarisatie ook de veiligheidsrisico's van het CSMS mee te nemen. Anders kan het CSMS de achilleshiel worden van de cybersecurity van de laadstations.

Uniformeer de eisen, bij voorkeur internationaal

Omdat verschillende marktpartijen uit de survey en interviews internationaal opereren is het van belang cybersecurity eisen internationaal op te stellen. Partijen stellen zelf voor dit minimaal op Europees niveau te doen. Door de eisen die in de verschillende landen gelden naast elkaar te leggen (zoals het Eichrecht voor Duitsland), ontstaat een redelijke complete set aan beveiligingseisen en door goede afspraken te maken worden tegenstrijdige eisen voorkomen.

De koplopersrol die Nederland ambieert is nodig om de continue ontwikkeling van cybersecurity voort te zetten. Landelijke regie is hierbij belangrijk, bij voorkeur door een organisatie die door alle stakeholders als voldoende onafhankelijk wordt ervaren. Die onafhankelijkheid is van belang om te voorkomen dat eisen die van belang zijn voor de ene groep stakeholders onevenredig zwaar wegen ten opzichte van de eisen die van belang zijn voor een andere groep. Bij de eisen die zijn opgesteld door ElaadNL ervaren sommige organisaties die medewerking hebben verleend aan deze inventarisatie te veel de nadruk op de netbeheerders.

Echter, door alleen voor Nederland eisen op te stellen die geen plaats krijgen in een internationale standaard, wordt Nederland mogelijk minder aantrekkelijk voor internationaal opererende marktpartijen. Dit dient tegen elkaar afgewogen te worden en parallel te worden opgepakt. Door dit te koppelen aan een heldere tijdlijn die aangeeft wanneer bepaalde beveiligingseisen geïmplementeerd moeten zijn, krijgen organisaties duidelijkheid over de benodigde investeringen. Dit maakt ook duidelijk hoe moet worden omgegaan met verouderde laadstations.

Creëer duidelijkheid over verantwoordelijkheden en toezicht

Op basis van een risico-inventarisatie kan inzichtelijk worden gemaakt wie welke risico's loopt, wie het meeste belang heeft bij een goede beveiliging om deze risico's weg te nemen of te reduceren en wie daar wat voor moet doen. Dit gaat verder dan alleen de belanghebbenden die deel hebben genomen aan deze inventarisatie, maar betreft ook netbeheerders, OEM's en EV-rijders. Het besef dat een goede beveiliging ieders verantwoordelijkheid is, draagt bij aan een eerlijk speelveld zolang de keuzes voor normen en standaarden breed gedragen worden.

Duidelijkheid over de beveiligingseisen en de verantwoordelijkheden van de betrokken organisaties vormt de eerste stap. Beveiliging heeft echter pas toegevoegde waarde op het moment dat dit frequent getoetst wordt om te zien of hier aan wordt voldaan. Een aanvullende aanbeveling is om op termijn de toetsing van deze eisen te beleggen. Hier kunnen binnen de sector afspraken over worden gemaakt of dit kan worden belegd bij een onafhankelijke organisatie. Zoals het Agentschap Telecom dit doet voor zendapparatuur, zou een onafhankelijke organisatie de autoriteit kunnen vormen voor het toetsen van laadstations. Afnemers van dergelijke laadstations kunnen er dan van uitgaan dat de laadstations voldoen aan de officiële normen en cybersecurity wordt op deze manier in de gehele keten geborgd.

Colofon

Opdrachtgever:	Nationale Agenda Laadinfrastructuur, Taakgroep Cyber Security
Datum:	29 april 2021
Auteurs:	Erik van Kreuningen Annabel van Zante (APPM Management Consultants)