34C3: Riesige Sicherheitslücken bei Stromtankstellen

27.12.2017 16:14 Uhr – Stefan Krempl

34C3: Umfangreiche Sicherheitslücken bei Stromtankstellen
(Bild: CC by 4.0 34C3 media.ccc.de))

An Ladesäulen auf fremde Rechnung Strom fürs E-Auto abzuzapfen ist laut dem Sicherheitsforscher Mathias Dalheimer kein Problem. Die Abrechnungsnummer für Nutzerkarten könne einfach kopiert werden, die Kommunikationsinfrastruktur sei kaum geschützt.

Die entstehende Infrastruktur öffentlicher Stromtankstellen geriet schon vor zwei Jahren ins Visier von Hackern aus dem Umfeld des Chaos Computer Clubs (CCC). Vieles sei "schon kaputt", hatte es damals geheißen. Der Sicherheitsforscher Mathias Dalheimer meldete nun am Mittwoch auf dem 34. Chaos Communication Congress (34C3) in Leipzig quasi Vollzug. "Die Anbieter haben grundlegende Sicherheitsmechanismen nicht umgesetzt³, erklärte das CCC-Mitglied. Wären die Lücken an der Kasse im Supermarkt genauso groß wie an den E-Zapfsäulen, könnte man dort "mit einer Fotokopie einer Girokarte" bezahlen und das ginge durch.

"Momentan sind Ladekarten und Abrechnungsprotokolle leider unsicher", betonte Dalheimer. Viele Stromtankstellen seien "trivial zu manipulieren". Hauptproblem sind laut dem Hacker bei allen Berührungspunkten mit der Infrastruktur zum Aufladen von E-Autos unzureichende Authentisierungsverfahren. Während etwa beim Online-Banking neben einer PIN zumindest eine TAN als zusätzlicher Faktor erforderlich sei, reiche bei Ladesäulen eine einzelne, einfach in die Finger zu bekommende Variable, um weitreichende Prozesse zu starten.

Mathias Dalheimer führte in Leipzig vor, wie einfach es ist, Strom aus öffentlichen Zapfstellen zu stibitzen.
Mathias Dalheimer führte in Leipzig vor, wie einfach es ist, Strom aus öffentlichen Zapfstellen zu stibitzen. (Bild: CC by 4.0 34C3 media.ccc.de))

Als Abrechnungslösung kommt an den derzeit über 11.000 hierzulande verfügbaren öffentlichen E-Zapfsäulen in der Regel das Open Charge Point Protocol (OCPP) in Version 1.5 von 2012 zum Einsatz. Er habe die entsprechende Spezifikation gelesen und nach 20 Minuten verstanden, dass die dabei

verwendeten Authentisierungsmechanismen unzureichend seien, berichtete Dalheimer, der am Fraunhofer-Institut für Techno- und Wirtschaftsmathematik (ITWM) in Kaiserslautern forscht. Ein "Token" in Form einer Abfolge von 20 Zeichen reiche aus, um mit dem Zentralsystem im Backend des Betreibers zu kommunizieren und Strom zu beziehen.

Völlig ungesichert

Dass das alles vergleichsweise einfach funktioniert, wenn man die Ladestation mit dem richtigen Wert füttert, zeigte Dalheimer in einem Video. Darin führte er vor, dass sich seine selbst gebaute "Testbox" in Form eines Auto-Adapters mit eigener Schutzleiterüberwachung und Laderegelung etwa auch ein Waffeleisen anschließen und bei den hierzulande vorherrschenden AC-Zapfsystemen "ganz normaler Wechselstrom" beziehen lasse. "Es gibt keine Signatur, keine Challenge, es wird nichts ausgehandelt", vermisste der Experte gängige Schutz- und Verschlüsselungsmechanismen.

Die erforderlichen Tokens seien ebenfalls leicht zu beziehen, erläuterte der Pfälzer. Die Ladekarten, auf denen diese gespeichert seien, könne man mit Lesegeräten wie Proxmark3 leicht inspizieren. Dabei habe sich herausgestellt, dass in der Regel Nahfunk-Karten mit "Mifare Classic"-Chips genutzt würden, obwohl schon seit rund zehn Jahren bekannt sei, dass deren Krypto-Implementierung große Löcher habe. Die Smart Cards könnten so auf triviale Weise komplett ausgelesen sowie über Zusatzwerkzeuge wie Chameleon Mini simuliert werden. Dabei habe er herausgefunden, dass als Authentisierungsmerkmal nur die Kartennummer verwendet werde. Habe man eine solche herausgefunden, lasse sie sich beliebig kopieren und etwa auf eine billige Blanko-Karte aus China übertragen.

Tanken auf Kosten anderer

Die Schwäche betreffe alle ihm bekannten Ladekartensysteme, unterstrich Dalheimer, neben dem Platzhirschen New Motion also etwa auch BMW Charge Now, E-Wald und Ladenetz. Bei diesen habe er getestet, dass in den Roaming-Protokollen für die übergreifende Abrechnung nur die eine Zeichenfolge als Authentisierungsmerkmal enthalten sei. Ein betrogener Nutzer kriege so im Zweifelsfall erst einen Monat später mit, dass Schindluder mit seiner Kartennummer betrieben worden sei.

Der Tüftler nahm auch konkrete Ladestationen der Hersteller Hager und Keba unter die Lupe und fand dort vergleichbare Angriffsflächen. Die Netzwerkkommunikation finde dort häufig "über http unverschlüsselt" statt, sodass jeder etwas erfahrene Hacker etwa mit dem Open-Source-Scanner Ngrep den Datenverkehr beobachten und die Ladenummern rauskopieren könne. Bei einer Verschlüsselung über https komme man mit einer "Man in the Middle"-Attacke weiter. E-Zapfsäulen seien auch übers Netz fernsteuerbar, man finde entsprechende Geräte über die aufs Internet der Dinge spezialisierte Suchmaschine Shodan. Dalheimer richtete ans Publikum aber die Bitte, solche offenen vernetzten Ladesäulen "in Ruhe zu lassen". Sonst könnte "im Zweifelsfall jemand nicht nach Hause fahren".

Steckt man an die USB-Buchsen der Haeger-Säule einen leeren USB-Stick, bekommt man von ihr die Konfigurationsdateien geschenkt.
Steckt man an die USB-Buchsen der Haeger-Säule einen leeren USB-Stick, bekommt man von ihr die Konfigurationsdateien geschenkt. (Bild: CC by 4.0 34C3 media.ccc.de))

Schraubendreher genügt

Recht leicht zu entdeckende USB-Ports für die Wartung der Geräte eröffnen dem Forscher zufolge weitere Spielwiesen für Hacker. Um an die Schnittstellen ranzukommen, müsse man im schwierigsten Fall ein paar Schrauben lösen. Stecke man bei Hager-Säulen einen eigenen leeren Stick

rein, liege hinterher eine Datei mit verräterischen Inhalten wie der Netzwerk-Konfiguration, Zugangsdaten und dem öffentlichen Endpunkt für OCPP-Server drauf. Dieses Geschenk müsse man nur noch der Anleitung entsprechend umbenennen - und schon werde es als neue Konfiguration mit den selbst vergebenen Berechtigungen für Manipulationen übernommen.

Bei Keba-Geräten könnten die Administratoren zwar verhindern, dass Konfigurationsdaten eingespielt würden, dafür würden weitergehende Software-Updates aber nicht verhindert. Die dazu benötigte Firmware, die sich modifizieren lasse, finde sich auf der Webseite des Herstellers. Dalheimer zeigte vor Ort und im Video, wie damit ein Skript von ihm ausgeführt wurde: Das Lademodul zeigte mit dem Hinweis "pwned" an, dass der Forscher sich Root-Zugang mit sämtlichen Berechtigungen verschafft hatte und so etwa signalisieren konnte: "Heute gratis laden." Ein Hacker sei so imstande, etwa die Kartennummern vorangegangener Fahrer zu extrahieren. Denkbar sei aber auch, dass der Ladesäulenbetreiber die Token selbst sammeln und über einen OCPP-Client Ladevorgänge simulieren und Nutzern in Rechnung stellen könnte.

Betreiber spielt Lücke herunter

Insgesamt fand Dalheimer "so offensichtliche Lücken, dass es eigentlich traurig ist". Die komplette Industrie sei betroffen, was der "ganzen Elektromobilität nicht gut tut". Das niederländische Fastned-System zum automatischen Laden von ABB nehme etwa nur die MAC-Adresse des Fahrzeugs als Authentisierungsmerkmal. Auch bei den alternativ nutzbaren Handy-Apps sowie im Backend der zentralen Abrechnungssysteme sehe es vermutlich nicht besser aus.

Der Ladenetzbetreiber New Motion hat in einer Stellungnahme in einem Onlne-Forum zwar die Möglichkeit eingeräumt, dass Ladekarten kopiert werden könnten. Bisher sei bei dem Verbund aber "kein einziger Fall von Kartenbetrug bekannt" geworden. Dies liege vermutlich auch daran, dass die Ladekosten, die derzeit bei maximal knapp 20 Euro pro 100 Kilometer liegen, niedrig seien. Betrug könne zudem "sehr einfach aufgedeckt werden", da ein Fahrzeug durchschnittlich mindestens 30 Minuten lang an der Ladestation parke. In dieser Zeit lasse sich genau nachvollziehen, welche Ladekarte gerade eingesetzt werde. Karteninhaber könnten sich zudem automatisch eine Nachricht auf Ihr Smartphone senden lassen, sobald auf ihr Konto zugegriffen werde.

Der CCC fordert, dass "die Sicherheit von Ladesäulen endlich auf den Stand der Technik gebracht werden muss". Ladenetzbetreiber sollten ihren Kunden sichere Bezahlmöglichkeiten bieten. Dafür müssten die Abrechnungsdaten nicht nur innerhalb eines Ladeverbundes, sondern auch beim Roaming zwischen verschiedenen Anbietern geschützt werden.

Eine Aufzeichnung des Vortrags kann vom Media-Server des CCC abgerufen werden.

(Stefan Krempl) / (hag)www.heise.de