woxx | 12 01 2018 | Nr 1458

REGARDS

THEMA

ELEKTROMOBILITÄT

Auf fremde Rechnung

Joël Adami

Immer mehr Ladestationen für Elektroautos werden in Luxemburg gebaut. Doch die verwendete Technik hat Schwächen.

Im Rahmen des Luxemburger „Autofestivals“ wird einmal im Jahr der motorisierte Individualverkehr mit beinahe religiösem Eifer zelebriert. Die Gretchenfrage war dabei lange Zeit „Diesel oder Benziner?“, doch inzwischen konvertieren immer mehr Autokäufer*innen zum Elektroantrieb. Lange Zeit wurden Elektroautos in Luxemburg von der Politik eher ignoriert. Die Finanzkrise änderte das; im Zuge eines Konjunkturprogramms wurden damals Prämien für den Kauf von PKWs mit Elektroantrieb gewährt. Eine konkrete Zielsetzung, wieviel Prozent des Fuhrparks nicht mehr mit Verbrennungsmotoren ausgestattet sein sollten, wurde allerdings nicht formuliert. 2014 lief die „Car-e“-Prämie aus, und es hatte den Anschein, als würde das Großherzogtum nicht beim Hype um Elektroautos mitmachen, der andere europäische Regierungen erfasst hatte. Doch zwei Jahre später sah die Welt schon wieder ganz anders aus. Einmal war da die Steuerreform, die, als „ökologisches Element“, eine Förderung für Elektroautos und -fahrräder vorsah. Statt einer Prämie bot die Regierung nun bis zu 5.000 Euro Steuererleichterung für den Kauf eines Elektroautos. Mittlerweile können auch die Käufer*innen von Hybridfahrzeugen, deren Akku an der Steckdose (Plug-in-Hybrid) geladen werden kann, von 2.500 Euro Steuerbonus profitieren. Musste für die „Car-e“-Prämie noch der Bezug von Strom aus erneuerbaren Energien nachgewiesen werden, so reicht jetzt für den Steuernachlass der Kauf des Fahrzeugs.

Visionen und Realität

Wurde 2016 auch die Studie zur dritten industriellen Revolution in Luxemburg vorgelegt, die im Rahmen des Rifkin-Prozesses erstellt worden war. Diese formulierte erstmals quanitative Ziele für die Elektromobilität im Großherzogtum. Bis 2050 sollen alle PKWs und Busse im Land einen Elektro-Antrieb besitzen, und schon ab 2025 sollen nur noch Fahrzeuge dieser Antriebsart zugelassen werden. Laut einer Schätzung des „Luxembourg Institute of Technology“ (LIST) könnten 2020 schon 40.000 Elektrofahrzeuge auf den hiesigen Straßen unterwegs sein.

Ein Blick in die Fahrzeugstatistik des Statec zeigt, dass zwischen dieser Vision und der Realität noch eine sehr weite Lücke klafft. In den letzten Jahren ist die Zahl der Elektrofahrzeuge in beinahe allen Bereichen zwar gestiegen, im Vergleich mit Diesel- oder Benzinmotoren spielen sie aber nur eine marginale Rolle. Auf alle Fahrzeuge gerechnet, haben lediglich 0,22 Prozent

FOTO: CC-BY KARLIS DAMBRANS

Danger! Bei Ladestationen für Elektroautos ist nicht nur der Strom gefährlich

der Fahrzeugflotte einen Elektromotor. Unter den privat genutzten PKWs, die den Löwenanteil (43 Prozent) der Flotte ausmachen, befinden sich gerade einmal 533 Elektroautos. Allerdings bedeutet das gegenüber 2013 einen Anstieg um fast das Zehnfache. Bekanntester Produzent von Elektroautos ist wohl der US-amerikanische Konzern Tesla, der es 2017 auf Platz 34 der Hitliste der meistverkauften Automarken in Luxemburg schaffte – mit immerhin 155 Fahrzeugen. Damit liegt Tesla mit seinen Luxus-Elektroautos aber zum Beispiel hinter der Marke „Landrover“, die eigentlich nur treibstofffressende SUVs verkauft. Die einzigen Fahrzeuge, bei denen Elektromotoren tatsächlich eine kleine Rolle spielen, sind überraschendweise „Cycles à moteur auxiliaire“, also Mopeds. Zwei Prozent des Bestands sind hier elektrisch angetrieben, obwohl es hier keinerlei staatliche Prämien oder Steuerboni gibt.

Park & Charge

Elektrofahrzeuge haben einen großen Nachteil: Ihre Batterie hat nur eine sehr begrenzte Kapazität, wodurch ihre Reichweite im Vergleich mit Fahrzeugen mit Verbrennungsmotor stark beschränkt ist. Hinzu kommt, dass ein Aufladevorgang einige Zeit dauert – sofern er nicht über eine spezielle Schnellladesteckdose, hinter der ein entsprechender technischer Aufwand steckt, erledigt wird. Eine wichtige Voraussetzung für einen Umstieg auf Elektromobilität ist also eine möglichst flächendeckende Versorgung mit Ladeeinrichtungen. Eine eigene Ladestation in der Garage ist für die meisten Elektroautofahrer*innen sicherlich Pflicht, aber wenn es unterwegs keine Gelegenheit gibt, auf- oder nachzuladen, ist die Gefahr groß, auf dem Trockenen zu sitzen. Es gibt also einen Bedarf an Ladestationen auf öffentlichen Parkplätzen und in Parkhäusern. Bis 2020 sollen in Luxemburg davon ingesamt 800 mit zwei Anschlüssen ausgestattete gebaut werden, sodass ingesamt 1.600 Fahrzeuge gleichzeitig geladen werden können. Dabei wird die Hälfte der Ladestationen auf Park&Ride-Parkplätzen errichtet

Die 800 Ladestationen werden unter dem Label „Chargy“ gebaut und betrieben, hinter dem die Energieversorger Creos, Electris, Sudstrom und die Gemeinden Ettelbrück und Diekirch stecken. Obwohl das Netzwerk erst seit Juni letzten Jahres besteht, konnte Chargy am 5. Januar in Schifflingen seine 100. Ladestation einweihen. Zweihundert weitere sollen in diesem Jahr folgen. Obwohl die meisten davon im Zentrum und im Süden des Landes geplant sind, soll es 2020 in jeder Gemeinde zumindest eine Ladestation geben. Wenn andere Akteur*innen Ladestationen aufstellen, können diese ins Chargy-Netzwerk integriert werden. Wer elektromobil unterwegs ist und trotzdem manchmal mit dem Rad fährt oder dem öffentliche Verkehrsmittel benutzt (oder umgekehrt), kann heute schon sein Chargy-Guthaben mit der „mKaart“ benutzen. Das ist jenes lila Stück Plastik, auf das auch Tickets für den öffentlichen Transport oder der Zugang für die Fahrradboxen („mBox“) geladen werden können.

FOTO: CC-BY MATHIAS DALHEIMER

Mit der richtigen Ausrüstung lassen sich an den Ladestationen auch Waffeln backen.

Werden Diskussionen über Elektromobilität geführt, wird oft das Für-und-Wider der Antriebsart abgewogen und der nötige Mentalitätswechsel beim „Tanken“ sowie die unklare Lage über den Ressourcenverbrauch bei Herstellung von Fahrzeugen und des Stroms erörtert. Selten wird jedoch die IT-Sicherheit des Ladenetzes thematisiert. Dabei wäre dies dringend nötig. Beim diesjährigen Kongress des deutschen Chaos Computer Clubs, der alljährlich Ende Dezember stattfindet, hielt Mathias Dalheimer vom Fraunhofer-Institut für Techno- und Wirtschaftsmathematik in Karlsruheeinen Vortrag über die Schwächen von Elektroauto-Ladeinfrastruktur. Er zeigte in diesem auf, wie leicht die Karten des Anbieters „New Motion“ ausgelesen und kopiert werden können: Das „kontaktlose“ Bezahlen mit Plastikkarte beruht auf der NFC-Technik (Near-field communication – Nahfeldkommunikation). Der Chip, der sich in der Karte versteckt, benötigt keine eigene Stromquelle, sondern wird mittels elektromagnetischem Feld von einem Ladegerät versorgt. Dalheimer kopierte für seinen Test nur seine eigene Karte – den Strom, den er mit der „Fälschung“ bezog, be-

THEMA

FOTO: PIXABAY

Über 100 Teslas sind auf Luxemburgs Straßen unterwegs, auch sie müssen regelmäßig Strom tanken.

zahlte er selbst. Zur Identifikation benutzt der deutsche Ladenetzbetreiber, eine weder durch Passwort, noch PIN oder Verschlüsselung geschützte ID-Nummer. Auf seinem Blog beschreibt Dalheimer, wie einfach es ist, solche Kartennummern zu erraten - innerhalb weniger Minuten wäre es leicht möglich, auf Kosten anderer Strom zu tanken.

Ist so ein Szenario auch in Luxemburg vorstellbar? Das Vorgängersystem der mKaart, das „eGo"-System, war alles andere als sicher. Damals war es mit ein wenig Fachwissen problemlos möglich, eine Fahrkarte zu kopieren. Nach dem Benutzen eines Tagestickets konnte dieses wieder auf den Chip geladen werden, sodass Hacker*innen sich mit etwas Aufwand sehr günstig eine „Jahreskarte" basteln konnten. Das New Motion-System basiert auf dem „Mifare classic"-Chip, während auf der mKaart in Luxemburg der neuere „Mifare DESFire EV1" zum Einsatz kommt, wie die Mobilitätszentrale der woxx auf Anfrage mitteilte. Dieser Chip ist wesentlich sicherer als sein Vorgänger, und bisher ist es nicht gelungen, seine Verschlüsselung zu knacken - 2016 haben jedoch zwei Forscher von der University of Kent Schwachstellen gefunden. Bisher gibt es dafür noch keine praktischen Nutzungsmöglichkeiten. Allerdings ist es möglich, die Karte zu emulieren, also mit Spezialgeräten wie dem „ChameleonMini" einem Lesegerät einen solchen Chip vorzugaukeln.

Obskure Sicherheit

Vielleicht ist es aber auch gar nicht nötig, das luxemburgische System zu knacken, um auf Kosten anderer zu tanken. Das Chargy-Netzwerk unterstützt nämlich Roaming mit dem New Motion-System. Die Karten anderer Ladenetzwerke können europaweit benutzt werden, sofern es ein Roamingabkommen zwischen den Anbietern gibt - was definitiv notwendig ist, wenn Elektromobilität auch grenzüberschreitend gelingen soll. Chargy ermöglicht es externen Anbieter*innen, zum Beispiel Supermärkten, die ihren Kund*innen Stromtankstellen zur Verfügung stellen wollen, Ladegeräte in sein Netzwerk einzubinden. Ein Blick auf die Spezifikationen der kompatibeln Ladesäulen zeigt, dass diese auch die unsicheren „Mifare classic"-Chips lesen können müssen. Auf der Seite goingeletric.de, auf der Elektroauto-Fans sich austauschen, ist die Roaming-Möglichkeit des luxemburgischen Ladenetzwerkes zu New Motion ebenfalls angegeben. Creos sagt dazu lediglich „Wir kennen das System von New Motion nicht." Wer nun denkt, dass Besitzer*innen von Elektroautos vermutlich sowieso genug Geld haben, um nicht auf Kosten anderer laden zu müssen, liegt vielleicht gar nicht so falsch. Mathias Dalheimer hat allerdings auch einen Elektroauto-Simulator gebaut, mit dem er einer Ladesäule ein Fahrzeug vortäuschen und jedes andere Gerät über die Ladesäule mit Strom versorgen kann. In einem Video ist der Forscher zu sehen, wie er auf einem öffentlichen Parkplatz ein Waffeleisen auspackt und mit dem Strom aus der Ladestation Waffeln backt. New Motion reagierte auf die Aufdeckung der Schwachstelle in ihrem System mit der Aussage, dass Betrugsversuche leicht erkennbar wären - Sicherheitsverbesserungen sind jedoch nicht geplant.

Grundsätzlich stellt sich die Frage, ob die Daten auf der mKaart oder der Chargy-Ladekarte überhaupt verschlüsselt sind. Die Nutzer*innen werden nämlich auch in Luxemburg nur mit einer Identifikationsnummer vom System erkannt, ein zweiter Faktor wie Passwort oder Pin ist nicht erforderlich. Das liegt allerdings nicht unbedingt an Chargy, sondern an den Protokollen, die zur Abrechnung und zum Roaming benutzt werden. Die verschiedenen Ladenetzbetreiber müssen die Informationen darüber, wer an welcher Tankstelle wieviel Strom geladen hat, austauschen. Zur Abrechnung verwendet Chargy das Open Charge Point Protocol (OCPP). Dalheimer hat sich auch dieses Protokoll angeschaut und festgestellt, dass die verwendeten ID nicht verschlüsselt oder signiert werden - die unsichere Authentifizierung hat also System. Außerdem ist der Datentransfer standardmäßig nicht verschlüsselt - wer also Zugriff auf das Netzwerk hat, in dem die Ladesäulen mit ihrer Zentrale kommunizieren, kann Kartennummern abfangen. „Wir wissen nicht genau, wie die Sicherheits des Protokolls ist, aber da wir in einem privaten APN kommunizieren, sollte es ziemlich schwer sein, die Kommunikation abzufangen", sagte Chargy dazu zur woxx. Ein APN ist ein mobiles Netzwerk, wie es auch auf Smartphones genutzt wird. In den Ladestationen steckt also eine Mobilfunkkarte, die die Netzwerkverbindung sicherstellt. Wie sicher es ist, sich auf die „Privatheit" des eigenen Mobilfunknetzes zu verlassen, darüber lässt sich streiten. Auch Mobilfunknetze sind hackbar - es wäre also durchaus denkbar, dass die Kommunikation zwischen Ladesäule und Zentrale abgehört oder gar manipuliert wird. In der Vergangenheit zeigte sich immer wieder, dass das Prinzip Security through obscurity (Sicherheit durch Obskurität) der Realität nicht standhält.

Zum Schluss sah sich Dalheimer auch noch die Sicherheit der Ladesäulen selbst an und stellte dabei fest, dass die in Deutschland populären Modelle leicht zu manipulieren sind: aufschrauben und einen USB-Stick einsetzen. Damit lässt sich die Firmware, das Betriebssystem der Ladesäule, manipulieren. Die Modelle, die in Luxemburg eingesetzt werden, sind jedoch nicht betroffen: „Die Chargy-Ladesäulen haben keinen USB-Port. Es wäre zwar möglich, eine physische Verbindung aufzubauen, dafür müsste man allerdings ein Schloss auf der Rückseite aufbrechen", heißt es bei Creos.

Die luxemburgischen Hacker*innen sind auf jeden Fall neugierig. „Das Thema steht bei uns auf dem Programm. Einen detaillierten Einblick in Technik und Funktionsweise können wir allerdings erst bieten, wenn wir uns näher damit auseinandergesetzt haben", verrät Sam Grüneisen vom C3L, dem luxemburgischen Ableger des Chaos Computer Clubs.

Wenn über die Zukunft der Mobilität und der Arbeitswelt im Rahmen der „dritten industriellen Revolution" gesprochen wird, wird der Faktor IT-Sicherheit meist vernachlässigt. Gerade im Rahmen einer dezentralisierten Energieversorgung verändert sich das Sicherheitsproblem von Ladestationen. Wenn Elektroautos als „fahrende Batterien" genutzt werden sollen - zum Beispiel um Engpässe zu überbrücken, wenn gerade keine Sonne scheint oder kein Wind weht -, dann kann aus dem Gratistanken-Betrug schnell eine Bedrohung der Sicherheit der nationalen Stromversorgung werden.