Virenschutz für Wallbox und Auto

Sicherheit | Elektroautos und Ladestationen sind meist mit dem Internet verbunden. Wie anfällig sind die Komponenten für Kriminelle? Braucht man hierfür eine Firewall? Die Antwort darauf ist recht leicht umzusetzen.

Was nur den wenigsten bekannt sein dürfte: Elektrofahrzeuge und Ladestation(en) bieten unter Umständen ein Einfallstor für Cyber-Kriminelle. Ist deswegen ein Virenschutz für E-Autos und die Wallbox notwendig? Diese Frage haben wir Thomas Köhler gestellt. Der Wissenschaftler tritt regelmäßig als Experte für IT-Themen in den Medien auf und sagt: „Je mehr ein Fahrzeug mit Software ausgestattet und vernetzt ist, desto größer ist das Risiko. Wir müssen davon ausgehen, dass es bereits einige Hackerangriffe auf E-Autos und Ladestationen gegeben hat." Konkrete Beweise dafür versuche man gerade zu ermitteln. Einen Virenschutz, wie man ihn von Computer oder Smartphone kennt, braucht der Endkunde laut Köhler aber nicht. Cyber-Sicherheit sollte aber schon ab Werk in die Software integriert sein.

Potenziell gefährdet

Mit dem Internet verbundene Geräte sind potenziell gefährdet. „Die Zugriffsmöglichkeiten für Kriminelle sind denkbar vielfältig", berichtet Köhler. „So könnten Hacker beispielsweise das Fahrzeug am Start hindern oder die Abrechnung der Wallbox manipulieren. Grundsätzlich muss man sagen, dass die Ladestation der größte Schwachpunkt in dem ganzen System ist", so der Experte. Hier fragen wir bei Christoph Erni nach. Erni ist CEO der Juice Technology AG, eines Ladeinfrastruktur-Anbieters aus der Schweiz, bei dem Thomas Köhler übrigens im Verwaltungsrat sitzt. Erni warnt vor noch größeren Folgen, die Cyberangriffe nach sich ziehen können: „Wird beispielsweise das Lastmanagementsystem eines Gebäudes gehackt, können Kriminelle bewusst Blackouts verursachen und so den Eigentümer erpressen. Theoretisch können mit der Kontrolle des Stromnetzes ganze Firmen oder gar Länder von Betrügern unter Druck gesetzt werden."

Wie sicher sind Wallboxen?

Nun stellt sich die Frage, wie wahrscheinlich solch ein Szenario ist. Grundsätzlich, da sind sich die handelnden Personen bei Juice Technology einig, steigt die Gefahr mit der Verbreitung der Systeme an. Denn je größer das Netzwerk, desto interessanter wird es für Kriminelle. Die hauseigenen Ladestationen werden deshalb nach einem sogenannten 3-Level-Security-Concept entwickelt. „Das heißt, wir müssen gewährleisten, dass das Gerät physisch, in der Anwendung und softwareseitig sicher ist", erklärt Erni. Der Virenschutz, den sich der Nutzer nicht selbst zulegen kann, ist gewissermaßen ab Werk programmiert und wird dann mit jedem Update erneuert. Es hängt also maßgeblich vom Hersteller oder Anbieter ab, wie sicher das System ist.

„Grundsätzlich ist das Bestreben der Anbieter, eine 100-prozentig sichere Lösung anzubieten, die zudem leicht in der Handhabung ist", sagt Erni. Gerade deshalb spüre man einen gewissen Druck, denn nur eine übersehene Lücke könnte schon dazu führen, dass das System angreifbar ist. Regelmäßige Updates sind deshalb unerlässlich, um mögliche Einfallstore schnell wieder zu schließen. Als Kunde kann man – egal ob E-Auto- oder Wallbox-Nutzer – nur wenig ausrichten.

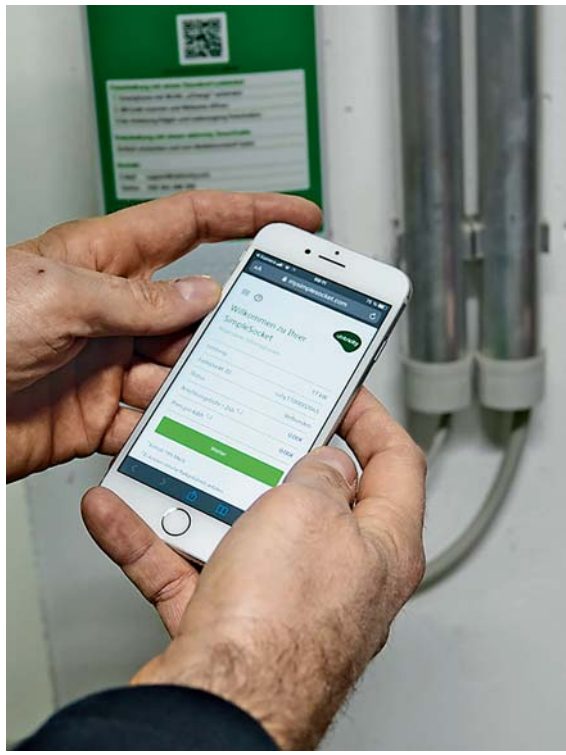

Foto: Rocco Swantusch/Autoflotte

Der Zugriff auf den Ladepunkt erfolgt oft per Handy, was ihn anfällig macht.

„Sie müssen im Grunde nur sicherstellen, dass Sie regelmäßig die Updates des Herstellers installieren", sagt Thomas Köhler. Dann sei man auf der sicheren Seite unterwegs. Dem Cyber-Experten zufolge kann der Kunde nur schwer erkennen, ob man gefährdet ist oder nicht.

Er rate deshalb sicherheitshalber regelmäßig die Abrechnungen zu kontrollieren. Bei Unregelmäßigkeiten solle sich der Nutzer dann direkt an die Polizei wenden. Der Experte empfiehlt darüber hinaus auch, im Falle des Falles direkt den Abrechnungsdienstleister zu kontaktieren, um zumindest einen potenziellen finanziellen Schaden abzuwenden.

Fabian Faehrmann

Kurzfassung

Elektroautos und Wallboxen können aufgrund ihrer Vernetzung und Internet-Anbindung ein Angriffsziel für Hacker sein. Die Hersteller müssen deshalb die Cybersecurity sicherstellen und Updates aufspielen.