Öffnet der Ladestecker Cyberkriminellen Tür und Tor?

Moderne Autos enthalten inzwischen teilweise Millionen von Codezeilen in ihrer Software und Sensorik. Die Software in der Automobilindustrie war noch nie so komplex wie heute. Die Herausforderung besteht nun darin, dies alles auch gegen Angriffe von außen abzusichern, damit aus Cyberrisiken keine für Leib und Leben werden. Beispiel Elektromobilität: Zum Elektroauto gehört die Ladesäule. Auch die kann zum Sicherheitsrisiko für alle werden. Darauf weist Thomas Ernst hin, „Security Evangelist“ bei Check Point Software Technologies in Tel Aviv, ein für Firewalls und Produkte zum Schutz von Virtual Private Network. (VPN) bekanntes Unternehmen.

Thomas Ernst warnt vor einer rasanten Expansion der Risiken, denn überall auf der Welt tauchten neue auf. Die neuen Installationen könnten jedoch Cyber-Angreifer dazu veranlassen, die Ladenetzwerke, die Fahrzeuge selbst und die angeschlossenen Stromnetze ins Visier zu nehmen, meint Ernst.

Bei vielen vernetzten Geräten hat das Wettrennen um die Markteinführung dazu geführt, dass Maßnahmen zur Cybersicherheit nur „aufgeschraubt“, aber nicht eingebaut wurden. Ernst: „Mit anderen Worten: Die Cybersicherheit wurde größtenteils nachträglich eingebaut. Im Fall von Ladestationen für Elektrofahrzeuge ist dies eine besonders beunruhigende Aussicht, da die Ladestationen mit anderen Infrastrukturen vernetzt sind.“

Ladestationen verbinden Transport und Stromnetz

Das National Institute of Standards and Technology (NIST) hat sich zum Ausmaß der Cybersicherheitsprobleme im Zusammenhang mit Ladestationen für Elektrofahrzeuge geäußert: „EVSE (Electric Vehicle Supply Equipment) wird von Elektronik unterstützt, sowohl für das Aufladen des Fahrzeugs, als auch für die Kommunikation, so dass EVSE anfällig für Schwachstellen bei der Cybersicherheit und für Angriffe ist. EVSE verbindet außerdem zwei kritische Sektoren – Transport und Energie (besonders das Stromnetz) –, die bisher nicht elektronisch miteinander verbunden waren.

Aus der Ferne „den Hahn zudrehen“

Cyberangriffe, die Schwachstellen von Ladestationen ausnutzen, könnten zu Stromschwankungen und Stromausfällen, den sogenannten Blackouts führen, Cyberangriffe könnten aber auch nur die Ladeinfrastruktur komplett lahmlegen, so dass Autofahrer gestrandet wären, warnt Ernst. Die genannten Beispiele sind für ihn nur einige der „unangenehmen Szenarien, über die Forscher im Bereich der Cybersicherheit und der Versorgungseinrichtungen für Elektrofahrzeuge geschrieben haben“. Einige sind bereits auf Schwachstellen gestoßen, die es Cyberkriminellen ermöglichen könnten, Ladegeräte für Elektrofahrzeuge aus der Ferne abzuschalten oder Strom zu stehlen.

Vier Empfehlungen zur Sicherheit

Mit den folgenden vier Empfehlungen gibt Thomas Ernst einen Überblick über die Möglichkeiten EV abzusichern:

Segmentierung von Netzwerk und Hardware: „Die Branche sollte nur vertrauenswürdige Komponenten einsetzen und eine partitionierte Architektur schaffen. Auf diese Weise würde eine Kompromittierung in einem Bereich nicht zwangsläufig zu einer seitlichen Gefahr für einen angrenzenden Bereich werden.“

Software-Sicherheit: „Die Unternehmen im Ökosystem der Elektrofahrzeuge müssen sichere Software verwenden. Die Umsetzung des Prinzips der geringsten Rechte ist von zentraler Bedeutung, da es gewährleistet, dass die Software nach dem Least Privilege-Prinzip arbeitet.“ Dasbei wir einem Benutzer nur das Minimum an Privilegien oder Zugriffsrechten gewährt, das für die Ausführung seiner Aufgabe erforderlich ist.

Etablieren eines Incident Response Prozesses: „Hersteller von Elektrofahrzeugen sollten ihre Systeme kontinuierlich auf Cyber-Aktivitäten überwachen und auf das Auftreten von Cyber-Bedrohungen vorbereitet sein. Unternehmen sollten außerdem MDR/MPR-Lösungen in Betracht ziehen.“ MDR/MPR (Managed Prevention & Response) überwacht, erkennt, untersucht, verfolgt, reagiert auf und beseitigt Angriffe auf Ihre Umgebung.

Sicherheit einbauen, anstatt sie nachträglich zu implementieren: „Die Cybersicherheit muss in die Software, den Hardware-Einsatz und andere Abläufe integriert werden. Darüber hinaus muss bei der Diskussion über Cyber-Risiken auch der menschliche Faktor berücksichtigt werden. So müssen beispielsweise Techniker ordnungsgemäß geschult und autorisiert werden, bevor sie sich mit der Infrastruktur befassen.“ (aum)

Bilder zum Artikel

An fehlenden Ladestationen darf die E-Mobilität nicht scheitern.

Foto: Auto-Medienportal.Net/Audi

Eon und die ADAC Service GmbH bieten ab sofort gemeinsam Ladestationen für Unternehmen an.

Foto: Autoren-Union Mobilität/Eon/Malte Braun

Schnellladestationen an der Autobahn.

Foto: Autoren-Union Mobilität/Tank&Rast