Dem vernetzten Auto können Hacker gefährlich werden

Seitdem sich Autos immer mehr in Richtung „rollende Computer“ entwickeln, wie manche meinen, wächst auch dort die Gefahr von so genannter Cyberkriminalität. Das Schreckensszenario für Autofahrer würde in einem solchen Fall bedeuten, dass Hacker das Fahrzeug manipulieren, es lahmlegen oder ganz unter ihre Kontrolle bringen. Ein solcher Missbrauch durch Fahrzeughacker schreckt viele Autofahrer ab.

Mehr Sicherheit ist eines der gewichtigsten Argumente für die vernetzten, automatisierten Autos, bemerkt das Goslar Institut für verbrauchergerechtes Versichern. Ebendiese Vernetzung stelle bei modernen Fahrzeugen aber auch eine erhebliche Schwachstelle dar, wie Experten erläutern. Konkret sind es demnach die Schnittstellen, über die Daten ausgetauscht werden, die Hackern den Zugang zu den Systemen ermöglichen. Aber ohne Vernetzung funktioniert die moderne IT im Auto nun einmal nicht. Beispiel E-Call: Das seit 2018 für alle Neuwagen vorgeschriebene automatische Notrufsystem stellt nach einem Unfall selbsttätig eine Verbindung zur nächsten Rettungsleitstelle her und fordert Hilfe an. Dabei werden als Informationen für die Retter unter anderem der Zeitpunkt des Unfalls, die Fahrzeugidentifizierungsnummer (FIN), die Position des Fahrzeugs, seine Fahrtrichtung und bei angelegten Sicherheitsgurten auch die Anzahl der Insassen übermittelt. Dazu nutzt der automatische Notruf Mobilfunk und Satellitenortung, aber eben auch die vom Fahrzeug erhobenen Daten.

Die Zukunft des Autos, das autonome Fahren, ist ohne solche Verbindungen gar nicht denkbar. Denn hochautomatisiert oder autonom fahrende Pkw müssen über leistungsstarke Schnittstellen permanent mit dem Internet, anderen Autos, der Umgebung und Satelliten verbunden sein, wie der ADAC erläutert. Das soll den Systemen im Auto ermöglichen, auf Gefahren zu reagieren und sich auf das Verhalten anderer Verkehrsteilnehmer einzustellen. Dies geschieht über schnelle Mobilfunknetze. Und so wie Hacker heute schon Daten von Handys und Computern klauen oder sich unberechtigt Zugang zu Systemen verschaffen, wo sie nichts zu suchen haben, besteht diese Gefahr eben auch bei den immer stärker vernetzten Fahrzeugen.

Mögliche Ansatzpunkte für Hacker sind nach Auskunft von Experten grundsätzlich alle Schnittstellen im Auto, also alle Verbindungen, über die Daten mit den Steuergeräten ausgetauscht werden. Das können Schnittstellen des fahrzeugeigenen Diagnosesystems sein, das wichtige Steuergeräte überwacht, das kann der so genannte Diagnosestecker sein, über den die Werkstatt Informationen über Fehlfunktionen erhält, das können selbst die Steuergeräte für die Wegfahrsperre sein. Und da in den modernen Autos die Zahl der Steuergeräte zunimmt, nehmen auch die möglichen Sicherheitslücken zu.

Steigt demnach mit der Vernetzung die Gefahr von Hackerattacken? Ja, sagt der ADAC. Begründung: Ein Auto, das permanent online ist, kann genauso zum Ziel von Hackern werden wie jeder PC, jedes Handy, jedes Gerät, das am Internet hängt. Deshalb fordern die Fachleute die Automobilhersteller und -zulieferer auf, für ein Höchstmaß an Cybersicherheit im Auto zu sorgen. Doch da dies mit relativ hohen Kosten verbunden ist, befürchtet nicht nur der ADAC, dass die Autohersteller dazu tendieren werden, vor allem unter wirtschaftlichen Aspekten abzuwägen, wie viel digitale Sicherheit sie ins Auto einbauen. Und diese Entscheidung dürfte eher zuungunsten der Sicherheit ausfallen, argwöhnt der Automobilclub.

Dabei haben IT-Spezialisten in den USA bereits im Jahr 2015 vorgeführt, wie real die Gefahr von Auto-Hacks bereits heute ist. Sie knackten einen Geländewagen, brachten das Auto unter ihre Kontrolle und lenkten ihn per Laptop in einen Graben. Auch die steigende

Zahl der Autodiebstähle, die auf Manipulationen der so genannten Keyless-Schlüsselsysteme zurückzuführen sind, spricht nach Ansicht der Experten zum Thema Sicherheit vor Hackerangriffen Bände. (ampnet/jri)

Bilder zum Artikel

Cyberkriminalität.

Foto: Auto-Medienportal.Net/Goslar Institut