# Wenn im Auto der Hacker das Kommando übernimmt

Von Walther Wuttke

Ihre Namen sind meistens unbekannt, ihre Adressen ebenfalls – und doch machen sie sich immer wieder spektakulär bemerkbar, wenn sie in fremde Rechner eingedrungen sind, Informationen stehlen oder Computernetze so manipulieren, dass sie nicht mehr zu benutzen sind. Hacker haben sich in den vergangenen Jahren zu einer wachsenden Bedrohung der Weltwirtschaft entwickelt und ganz nebenbei auch die klassischen Agenten à la James Bond ein Stück arbeitslos gemacht.

Der Spion von heute braucht keine Walther PPK mehr, er sitzt am Keyboard und sucht seinen Eintritt in die fremde Datenwelt, um dort seine Informationen zu sammeln. Die Automobilindustrie fürchtete Hacker bisher allenfalls als Bedrohung ihrer Entwicklungsabteilungen. Doch je mehr die einzelnen Automobile auf den Straßen sich zu rollenden Computern entwickeln, desto mehr geraten die elektronischen Attacken zu einem ernsten Problem. Höhepunkt war im vergangenen Jahr die Attacke auf die Elektronik eines Jeep Cherokee (Baujahr 2014), bei der aus der Entfernung die Automatik abgeschaltet wurde, die Fahrt im Straßengraben endete und Chrysler schließlich 1,4 Millionen Fahrzeuge in die Werkstätten rufen musste.

Wenig später demonstrierten Computer-Experten der University of California in San Diego, wie sich über einen Versicherungs-Dongle die Bremsen einer Corvette lahm legen ließen. Inzwischen hat sich auch die US-amerikanische Bundespolizei FBI mit dem Thema befasst und warnt die Fahrer vor Hacker-Attacken, denn je mehr vernetzte Fahrzeuge mit autonomen Funktionen auf die Straßen kommen, desto interessanter werden sie für Hacker.

Das FBI warnt die amerikanischen Autobesitzer konkret davor, keinem Außenstehenden Zugang zum Auto zu gestatten. „Genauso wenig wie sie Ihren PC oder ihr Smartphone offen herumliegen lassen würden, sollten sie sich genau darüber im Klaren sein, wem sie den Zugriff auf Ihr Fahrzeug gestatten“, heißt es in einer öffentlichen FBI-Warnung. Außerdem werden die Autobesitzer aufgefordert, keine unerlaubten Veränderungen an der Software vorzunehmen oder unsicheres Zubehör zu montieren oder zu installieren. Gleichzeitig sollen sich US-Bürger sofort mit dem FBI in Verbindung setzen, wenn sie glauben, dass ihr Fahrzeug von Hackern angegriffen wurde.

Insgesamt sind zurzeit knapp 112 Millionen vernetzte Fahrzeuge weltweit unterwegs (bei einem Bestand von mehr als einer Milliarde), die sich als Ziel für die internationale Hacker-Gemeinschaft anbieten. Nach Berechnungen des Analyse- und Informationsunternehmens IHS wird der Markt für Cybersicherheit bis zum Jahr 2023 auf einen globalen Umsatz von 759 Millionen US-Dollar wachsen. IHS definiert vernetzte Fahrzeuge als Modelle, die eine Verbindung mit dem Internet besitzen, die auch über ein Smartphone hergestellt sein kann.

Parallel zur elektronischen Aufrüstung der Fahrzeuge haben, so IHS, auch die Hacker dazugelernt und die digitalisierte und vernetzte Mobilität als Ziel definiert. Die Hersteller haben diese Gefahr erkannt und investieren daher zunehmend in Maßnahmen, um die Cybersicherheit der Fahrzeuge zu verbessern, sodass die Angriffe aus dem Netz abgewehrt werden können.

Nach einer Analyse von IHS wird sich der Markt für Cybersicherheit in zwei Segmente aufspalten. Zum einen wird eine entsprechende Schutzsoftware in den zahlreichen Rechnern und Datenbussen im Fahrzeug selbst installiert werden, um die verschiedenen

Funktionen von Airbags bis Benzinpumpe zu regulieren und zu kontrollieren. Die Computer werden so zu elektronischen Kontrolleinheiten. Als zweite vorbeugende Möglichkeit können Cybersicherheitsmaßnahmen in der Daten-Cloud dienen. Diese Dienste kontrollieren und steuern ganze Fahrzeugflotten mit ihrer Software und registrieren und verfolgen jede Unregelmäßigkeiten.

Im Jahr 2023 werden 25 Prozent der weltweit verkauften Fahrzeuge mit Cloud-Sicherheitssystemen ausgerüstet sein, schätzt IHS. Die meisten Fahrzeuge werden nach Einschätzung der Experten in Zukunft mehrere elektronische Kontrolleinheiten besitzen, wobei die Zahl auf 50 bis 60 steigen kann.

„Die Cybersicherheit wird in den kommenden Jahrzehnten eine der größten Herausforderungen für die Automobilindustrie sein“, erklärt IHS-Experte Colin Bird. „Vor allem, weil viele Fahrzeuge mit Telematik und eingebetteten Modems sich zu einem attraktiven Ziel für Cyber-Kriminelle und Terroristen entwickeln.“ Die USA und Westeuropa werden angesichts der Verbreitung vernetzter Autos nach der IHS-Analyse die führenden Märkte für diese Technologien werden. Das Jahr 2018 wird danach den größten Zuwachs verzeichnen, der danach etwas abnehmen wird. General Motors, BMW und Mercedes-Benz sind aktuell, so IHS, führend bei der Integration von Cybersicherheitslösungen in ihren Fahrzeugen.

„Cyber-Sicherheit wird sich angesichts der wachsenden Zahl von vernetzten Fahrzeugen zu einer Schlüssel-Technologie für die Automobilindustrie entwickeln“, erklärt Egil Juliussen, der an der Studie mitwirkte. Und: „Sie ist vor allem bei selbstfahrenden Automobilen von größter Bedeutung und muss dort unbedingt an Bord sein.“ (ampnet/ww)

## Bilder zum Artikel

Autonomes Fahren: Hände nicht am Lenkrad - noch lange illegal.

Foto: Auto-Medienportal.Net/Daimler