vmware®

Connected Car Business Brief Series | 02

SCHUTZ DER PRIVATSPHÄRE UND DATEN IM ZEITALTER DER CONNECTED CARS

Mit dem Zeitalter des Connected Car wird eine Fülle von neuen Möglichkeiten entstehen – leider jedoch auch genauso viele Risiken. Um Erfolg zu haben, müssen OEMs der Automobilindustrie die Sicherheit zur Priorität machen.

Im Juli 2015 machten die Sicherheitsexperten Charlie Miller und Chris Valasek Schlagzeilen, indem sie sich in ein fahrendes Auto hackten und die Kontrolle über das gesamte Fahrzeug übernahmen, von den Scheibenwischern bis hin zum Gaspedal. Die potenziellen Folgen sind offensichtlich, wenn nicht gar tödlich. Je vernetzter und softwareorientierter Fahrzeuge werden, desto größer die Wahrscheinlichkeit solcher Angriffe. Denn umso mehr Funktionen eines Fahrzeugs auf Software basieren, desto höher die Zahl der potenziellen Schwachstellen, die von Hackern ausgenutzt werden können. Wenngleich diese Art von Angriffen „in Bewegung" die größte Aufmerksamkeit der Medien bezüglich der Sicherheit von vernetzten und fahrerlosen Wagen auf sich lenken wird, müssen viele weitere potenzielle Risiken berücksichtigt werden.

Beispielsweise könnten Kriminelle versuchen, sich Zugriff auf Fahrzeuge zu verschaffen, nicht um sie zu kontrollieren, aber um geschützte oder sensible Daten von Herstellern, Anwendungsanbietern oder Fahrzeugbetreibern wie Transporteuren oder Kurierdiensten zu stehlen. Dies sollte den OEMs der Automobilindustrie ernsthaft zu denken geben, insbesondere vor dem Hintergrund des 53%igen Anstiegs der vom FBI im Juli 2015 berichteten Fälle der Industriespionage.[1]

Ein weiteres potenziell schädliches Szenario betrifft den Diebstahl personenbezogener Daten von einzelnen Fahrzeughaltern oder Benutzern. Beispielsweise haben viele Fahrer ihre Smartphones mit den integrierten Infotainment-Systemen per WLAN oder Bluetooth verbunden. Diese Geräte werden zunehmend zum Einkaufen verwendet und können daher wichtige Finanzdaten wie Kreditkartendetails enthalten. Außerdem übertragen sie fortlaufend Standortdaten, was von Arbeitgebern, Versicherungsunternehmen oder Privatdetektiven dazu genutzt werden könnte, um die Bewegungen eines Fahrers und sein Fahrverhalten nachzuweisen oder zu widerlegen. All diese Fälle begründen ernste Datenschutzprobleme, denen sich OEMs der Automobilindustrie bewusst sein müssen, um sich selbst vor Gerichtsverfahren und Schäden des Markenimages zu schützen. Hinzu kommt, dass sich die Vorschriften und Einstellungen gegenüber Datenschutz von Land zu Land erheblich unterscheiden, was das Ganze noch komplexer macht.

Im schlimmsten Fall könnte ein nicht effektiver Umgang mit diesen Problemen die Nachfrage der Verbraucher nach Fahrzeugen, Anwendungen oder Dienstleistungen, die als unsicher angesehen werden, schwächen. Die möglichen Folgen reichen von verfehlten Verkaufszielen bis hin zum Marktversagen von neuen Dienstleistungen oder Modellen.

In einer idealen Welt würden all diese Risiken durch eine umfassende Sicherheitsstrategie rund um Connected Cars vermieden werden, die die gesamte Lebensdauer des Fahrzeugs abdeckt – vom Design und der Herstellung über den Verkauf bis hin zur Nutzung und Entsorgung. Dadurch stellt sich die Frage, wie ein optimaler Ansatz für die Sicherheit von Connected Cars aussieht.

Durch VMwares Erfahrung und innovativen Ansatz im Hinblick auf Sicherheit für Rechenzentren, Head-Units in Fahrzeugen und drahtlose Netzwerke ist das Unternehmen perfekt aufgestellt, um diese Frage für Unternehmen für die gesamte Wertschöpfungskette der Connected Cars zu beantworten.

[1] FBI Pressebriefing, Juli 2015