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

HACKER FERNHALTEN – VON DER BEDROHUNG ZUR CHANCE

Es ist eines jeden Fahrers (und Herstellers) Albtraum: Die Kontrolle über ein Fahrzeug verlieren und Schäden oder Verletzungen aufgrund technischen Versagens erleiden. Erfreulicherweise sind moderne Fahrzeuge so gut gebaut und so zuverlässig, dass solche Ereignisse selten sind. Doch was, wenn ein scheinbares Versagen von außen initiiert und kontrolliert wurde?

Der kürzlich von zwei Sicherheitsexperten in den USA (siehe vorherige Seite) durchgeführte Hackangriff „in Bewegung" hat gezeigt, dass ein solcher Angriff möglich ist, und sie hatten vor zwei Jahren sogar schon einmal einen ähnlichen Coup gelandet. Der Unterschied zwischen diesen beiden Vorfällen? 2013 saßen sie in einem Fahrzeug, in dem ein Computer mit der Head-Unit physisch verbunden war. 2015 hackten sie sich entfernt in die Head-Unit, indem sie einen offenen Port für die Verbindung mit einem Mobilfunknetz über eine eingebettete SIM-Karte nutzten. Die potenziellen Folgen eines solchen Angriffs in der Realität sind klar: schwere Verletzungen oder Schlimmeres für die Insassen des Fahrzeugs und katastrophale Auswirkungen auf das Ansehen des Fahrzeugherstellers. Dies ist ein weiterer Beweis, falls es solcher überhaupt bedarf, für die potenziellen Gefahren in Zusammenhang mit zunehmend softwareorientierten Fahrzeugen. Hinzu kommt, dass „traditionelle" Hackerangriffe dieser Art längst nicht die einzige Bedrohung sind.

Ein Forschungsmitarbeiter an der University of Cork hat beispielsweise nachgewiesen, wie durch die Kombination eines Lasers (ähnlich wie die gewöhnlichen Laserstifte) mit einem Impulsgeber, der auf jedem Computer erstellt werden kann, den Lidar-Sensoren, mit denen fahrerlose Autos geführt werden, Objekte auf der Fahrbahn vorgegaukelt werden können, die in Wirklichkeit gar nicht existieren. In dem Test des Wissenschaftlers verlangsamte das Fahrzeug automatisch seine Geschwindigkeit, um nicht gegen diese Phantomobjekte zu fahren. Projiziert man genug dieser Objekte auf der Straße, würde das Fahrzeug komplett zum Stehen kommen.[2] Genauso wie das erste Beispiel hat auch dieser Vorfall das Potenzial für Schlagzeilen. Doch Hacker können auch auf viele andere Arten Schaden anrichten. Mögliche Gefahren sind:

- Fahrzeugdiebstahl oder elektronische Schäden/Blockierung
- Fälschung der Fahrzeuginformationen wie dem Kilometerstand
- Zugriff auf persönliche Informationen wie Telefonnummer, Adressbücher, Kreditkartendetails, Standortinformationen etc., die alle entweder direkt missbraucht oder zur Erpressung verwendet werden könnten
- Abhören von Sprach- und Datenkommunikation
- Zugriff auf geschützte Daten der Hersteller, Dienstleister oder App-Anbieter über die Head-Unit des Fahrzeugs

OEMs der Automobilindustrie müssen diesen Problemen eine sehr hohe Priorität einräumen, denn alles andere könnte erhebliche Auswirkungen auf das Interesse und die Nachfrage nach Connected Cars, fahrerlosen Autos und den damit verbundenen Vorteilen haben. Doch es gibt auch angenehme Aspekte, denen sich die Hersteller widmen können.

Anbieter, die die Herausforderungen beim Schutz von Connected Cars gründlich und skalierbar lösen können, haben durch die schnelle Markteinführung einen bedeutenden Vorteil gegenüber ihren Wettbewerbern. Wenn sie zudem die Überlegenheit ihrer Sicherheitslösungen demonstrieren können, verfügen sie über ein überzeugendes Alleinstellungsmerkmal, mit dem sie das Vertrauen der Kunden gewinnen und ihren Marktanteil ausbauen können.

VMware ist führend auf dem Gebiet der Containerisierung und Mikrosegmentierung, beides Maßnahmen, die die Sicherheit durch die Separation von Computerressourcen, Netzwerken und Daten verbessern und die potenziellen Folgen von Hackerangriffen minimieren. Nicht nur das: VMware versteht es, dieselbe Technologie sowohl im Rechenzentrum als auch im Fahrzeug einzusetzen, um den OEMs der Automobilindustrie einen Wettbewerbsvorteil im Zeitalter der Connected Cars zu verschaffen.

[2] Bericht von IEEE Spectrum, September 2015

VERTRAUEN AUFBAUEN FÜR CONNECTED CARS

Eine der größten Herausforderungen für den künftigen Erfolg von vernetzten und fahrerlosen Autos ist die Schwerfälligkeit und das Misstrauen der Kunden. Sogar „Digital Native“, die sich sonst weniger Gedanken über den Online-Datenschutz machen, werden es sich zweimal überlegen, bevor sie die Funktionen des Connected Car nutzen, wenn sie den Eindruck haben, dass dadurch ihre persönlichen Informationen oder die ihrer Familie und Freunde gefährdet werden.

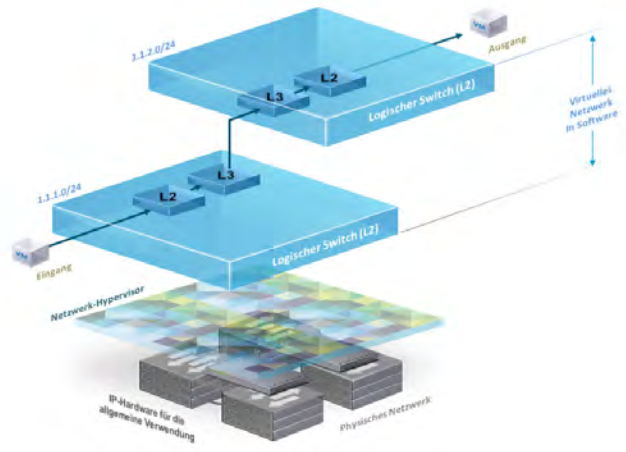
In diesem Zusammenhang ist ein wichtigstes Element für ein persönlicheres und vernetztes Erlebnis im Fahrzeug durch Apps oder Services die Garantie, dass die betroffenen persönlichen Daten privat bleiben. Gleichzeitig müssen auch Hersteller ihre eigenen Infrastrukturen und Daten vor Angriffen gegen Kunden und Fahrzeugnutzer schützen. Dazu könnte gehören, Fahrern die Nutzung potenziell unsicherer Anwendungen von Drittanbietern mit einer sicheren Fahrzeugsoftware oder in einer geschützten Netzwerkumgebung zu verwehren. Ebenso könnte verhindert werden, dass ein Fahrzeug vorsätzlich so verändert wird, dass Garantien oder Versicherungspolicen wirkungslos werden. Das Mindeste wäre die Erkennung solcher Manipulationen, auch wenn die Verantwortlichen versucht haben, ihre Spuren zu verwischen.

Mit dem Vormarsch des Carsharings möchten Hersteller von Connected Cars sowie Fuhrparkbesitzer möglicherweise das Fahrverhalten und die Routen kontrollieren und nachweisen, insbesondere wenn Einzelne extremes Fahrverhalten an den Tag legen, das Fahrzeugschäden oder Rechtsverstöße zur Folge hat.

Es ist klar, dass jeder Anbieter in der Wertschöpfungskette im Zeitalter der Connected Cars einen kontinuierlichen und schwierigen Balanceakt zwischen dem Schutz von Kundendaten einerseits und der Wahrung der Integrität und der Rückverfolgbarkeit der eigenen Daten andererseits vollführen muss. Diese Ausgewogenheit wird ausschlaggebend sein, um Streitigkeiten zu lösen und rechtliche Verpflichtungen einhalten zu können. Dafür ist ein flexibles Management erforderlich, um die Art und Häufigkeit der zu erfassenden Daten festzulegen. Beispielsweise dürfen manche Daten, die für prädiktive Analysen erforderlich sind, keinen Drittunternehmen verfügbar gemacht werden, wenn dadurch die unerlaubte/illegale Erstellung von Profilen über das Verhalten eines Fahrers ermöglicht wird.

VMware Airwatch verwendet branchenübliche Algorithmen und eine leistungsfähige Datenschutz-Engine, um in einem solchen Szenario die erforderliche Anpassung der gesammelten und gespeicherten Datentypen vorzunehmen. Nicht nur das: Der IoT-Agent der Head-Unit kann Daten in einem verschlüsselten Container speichern und diese über sichere Kanäle an das Rechenzentrum übertragen. Die Containerisierung ist eine etablierte Technologie im Enterprise Mobility Management zur Trennung der beruflichen von privaten Daten und kann ebenso für Herausforderungen im Bereich Sicherheit und Datenschutz in der gesamten Wertschöpfungskette eingesetzt werden.

Die NSX-Lösung von VMware ermöglicht die drei wichtigsten Funktionen der Mikrosegmentierung: die Isolierung von Netzwerken, Segmentierung der Kommunikationen und Unterstützung zahlreicher Sicherheitsprodukte externer Anbieter. Die gleichen Grundsätze können für das Fahrzeug übernommen werden, um einen höheres Maß an Schutz zu bieten.



Und als führendes Unternehmen in der Mikrosegmentierung (siehe Diagramm) kann VMware außerdem dafür sorgen, dass bei der Gefährdung einer Anwendung oder eines Systems alle anderen Systeme und Services davon unberührt bleiben. Damit ist VMware der am besten positionierte Anbieter, um Herstellern dabei zu helfen, Sicherheitsrisiken und Datenschutz/Compliance-Probleme zu minimieren, die im Zeitalter der Connected Cars unvermeidlich auftreten werden.

CONNECTED CAR BUSINESS BRIEF SERIES

In der VMware Connected Car Business Brief Series wird erklärt, wie VMware OEMs der Automobilindustrie beim Bau einer hoch skalierbaren und sicheren Infrastruktur für Connected Cars und fahrerlose Fahrzeuge unterstützt. In den Broschüren werden folgende Themen behandelt:

01 **Vision:** Förderung neuer Geschäftsmodelle in der Automobilbranche durch einen sicheren und effizienten Austausch von Daten und Informationen zwischen Fahrzeugen, Benutzern und Anbietern über die Cloud.

02 **Sicherheit:** Innovative segmentbasierte Sicherheits-konzepte in Rechenzentren, Head-Units und kabellosen Netzwerken, die Geschäftsrisiken minimieren und den Fahrer schützen.

03 **Over-the-Air-Software:** Sichere Erfassung, Analyse, Verwaltung und Übertragung von Echtzeitdaten, die über die Luftschnittstelle (Over-the-Air; OTA) zwischen Treibern, Head-Units und Anbietern übertragen werden.

04 **Erfassung und Analyse von Daten:** Optimale Nutzung der Daten des Connected Car mithilfe des Software-Defined Datacenter, sicherer öffentlicher Cloud-Infrastrukturen, cloudbasiertem Datenmanagement sowie intelligenter Device Agents im Fahrzeug.

05 **Neue Geschäftsmodelle:** Erschließung neuer Einkommensquellen durch Mehrfachnutzung von Daten, Fahrererlebnis on Demand, fahrerlose Transport-services und vieles mehr.

Die Connected-Car-Re-volution im Überblick — 01

02 Die Sicherheit im Zeitalter der Connected Cars

03 Verwaltung des „Geräts auf Rädern“

04 Nummer Eins im Rennen um die datengesteuerte Zukunft

05 Neue Einnahmequellen durch Connected Cars

Ihr Ansprechpartner

Matthias Schorer
Senior Manager Advisory und Professional Services Development, CEMEA

Matthias Schorer leitet das VMware Accelerate Advisory Services Team in Mittel- und Osteuropa seit 2012. Er verfügt über umfangreiche Kenntnisse in den Bereichen IT-Architektur, Migration veralteter Systeme, Cloud Computing und Virtualisierung in verschiedenen Branchen mit einem besonderen Schwerpunkt in der Automobilbranche und Connected-Car-Innovationen.

mschorer@vmware.com
Tel. +49 89 / 3706 17108

Informationen zu VMware

VMware ist ein führender Anbieter im Bereich Cloud-Infrastrukturen und mobile Unternehmenslösungen. Unsere Lösungen basieren auf der branchenführenden Virtualisierungstechnologie von VMware und liefern ein brandneues IT-Modell, das sich durch einen reibungslosen und unmittelbaren Betrieb und eine verbesserte Sicherheit auszeichnet. Da Anwendungen schneller entwickelt, automatisch bereitgestellt und sicherer genutzt werden können, lassen sich Innovationen innerhalb kürzester Zeit umsetzen. VMware verfügt über mehr als 500.000 Kunden und 75.000 Geschäftspartner und hat im Jahr 2014 einen Umsatz von 6 Milliarden US-Dollar erwirtschaftet. Der Hauptsitz von VMware befindet sich im Silicon Valley. Das Unternehmen verfügt über Niederlassungen auf der ganzen Welt und ist online unter **www.vmware.com** zu finden.

VMware Global, Inc. Zweigniederlassung
Deutschland

Freisinger Str. 3
85716 Unterschleißheim

www.vmware.com/de

1510