Link: https://www.cio.de/a/das-connected-car-braucht-sicherheit,2976549

Security bei der Cape to Cape Challenge 2014

Das "Connected Car" braucht Sicherheit

Datum: 12.11.2014
Autor(en): Sebastian Christe

Das Auto von heute ist vernetzt: mit der Service-Infrastruktur des Herstellers, aber auch mit mobilen Endgeräten, Apps und Cloud-Diensten des Fahrers. Damit der PKW nicht zum IT-Sicherheits- und Datenschutzrisiko wird, ist eine gesamtheitliche Sicherheitsarchitektur erforderlich.

Die Vernetzung moderner Fahrzeuge bewegt sich im Formel-1-Tempo voran. Nicht nur, dass die Automobilhersteller Motor- und Fahrzeugdaten mittels Bordcomputer aufbereiten und per Diagnosestecker auslesen; auch der Autokäufer legt heute großen Wert darauf, dass ein PKW in seinen digitalen Lifestyle passt: Er erwartet ein In-Vehicle-Infotainment- (IVI-) System, das sein Smartphone problemlos einbindet, ebenso sein digitales Adressbuch oder Cloud-Services wie Geolokations- und Verkehrsinformations- oder auch Musik-Streaming-Dienste. Der moderne Nutzer versteht das Smartphone wie auch das Auto als Erweiterung seiner Persönlichkeit, also haben beide nahtlos zu interagieren.

Im September begab sich Rekordfahrer Rainer Zietlow im Rahmen der „Cape to Cape Challenge 2014“ in seinem Connected Car auf die Fahrt um den halben Globus.
Foto: HP Deutschland

Von der zunehmenden Vernetzung der Fahrzeuge profitieren aber nicht nur der Hersteller und der Fahrzeughalter oder Fahrer: In manchen Ländern ist es heute schon üblich, das Kfz-Versicherungen ihren Kunden günstigere Tarife anbieten, wenn diese eine "Black Box" in ihr Fahrzeug montieren lassen, die kontinuierlich Informationen zum Fahrverhalten an den Versicherer übermittelt. Dies ebnet den Weg für Tarife, deren Höhe davon abhängt, wie vorschriftsmäßig der Versicherte sich im Straßenverkehr verhält.

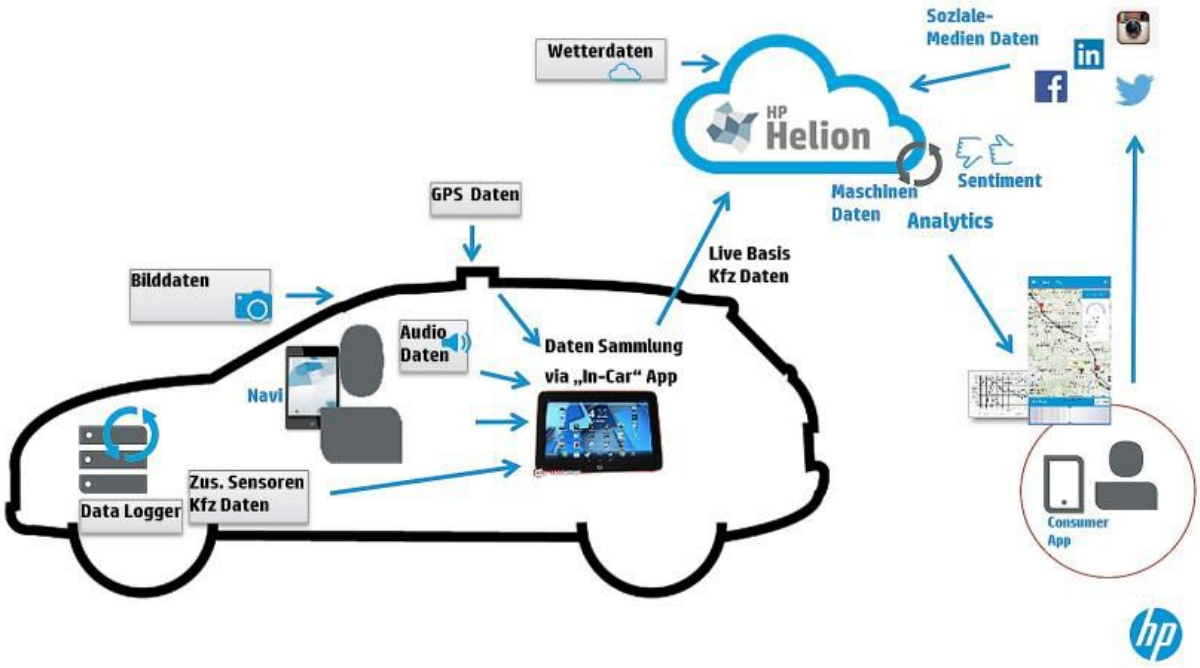
Überdies arbeiten der Internetkonzern Google wie auch zahlreiche Autohersteller am autonom fahrenden PKW. Ein Parkassistent, der am Straßenrand das lästige Einparken selbsttätig übernimmt, ist heute bei Herstellern wie Volkswagen bereits erhältlich - und selbst ein Auto, das sich im **Parkhaus seinen Stellplatz selbst sucht, ist technisch möglich**[1].

Googles fahrerloses Testfahrzeug [2]hat bereits über eine Million Kilometer unfallfrei zurückgelegt, und im Mai dieses Jahres hat der US-Konzern sogar einen "Driverless Car"-Prototypen vorgestellt, der weder **Lenkrad noch Gas- oder Bremspedal aufweist**[3]. Autonome PKW, die dem Fahrer das Fahren praktisch vollständig abnehmen, sind somit keine Science Fiction mehr.

Für den Nutzer, so das Versprechen der Branche, wird Mobilität damit entspannter, bequemer, dank intelligenter Echtzeit-Verkehrssteuerung zugleich schneller und durch das Wegfallen von Fahrfehlern und "Schrecksekunden" auch sicherer - von den volkswirtschaftlichen und versicherungstechnischen Vorteilen einer niedrigeren Unfallquote ganz zu schweigen.

Herausforderung Informations- und Datensicherheit

Die Vorteile immer stärker vernetzter - und letztlich gar autonomer - Fahrzeuge können aber nur zum Tragen kommen, wenn ein Höchstmaß an Informationssicherheit und Datenschutz garantiert ist. Auf Hackerkonferenzen wie der Black Hat in Las Vegas sind Angriffe auf Connected Cars längst ein gefragtes Thema: In Vorträgen wurde demonstriert, dass **Angriffe auf Fahrzeuge selbst namhafter Hersteller durchaus möglich sind**[4].



Bei der Cape to Cape Challenge erfolgte der Datenaustausch zwischen Zietlows Touareg, den HP Slate Tablets und der HP Helion Cloud durchgängig verschlüsselt.
Foto: HP Deutschland

Sicherheitslücken können sich bei den IT-Komponenten eines modernen Fahrzeugs unter anderem durch fehlerhafte Programmierung, unzureichende Systemhärtung und in der Folge durch Zero-Day-Angriffe ergeben. Hier gilt es, Schwachstellen zu unterbinden, damit die Verkehrssicherheit eines vernetzten Fahrzeugs nicht durch mangelnde IT-Sicherheit gefährdet wird.

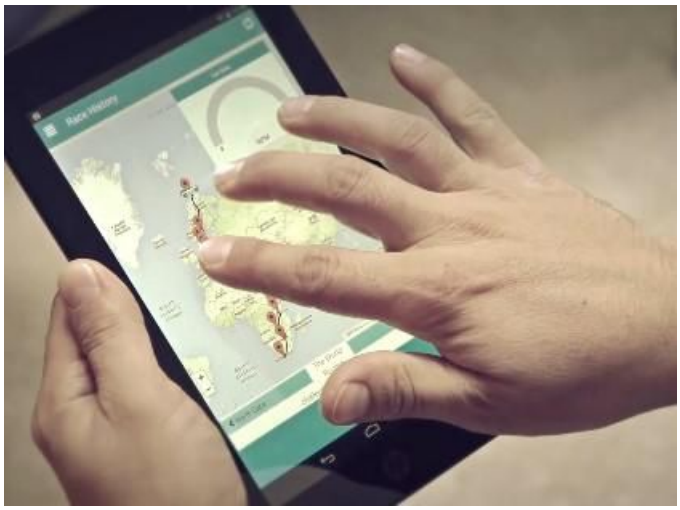
Ebenso muss sichergestellt sein, dass bei den Daten, die während einer Autofahrt über Fahrer und Fahrzeug anfallen, der Datenschutz gewahrt bleibt. Die Diagnose eines Pannenfahrzeugs mittels Bordcomputer spart Zeit, doch die ausgelesenen Daten sollen ausschließlich der Fachwerkstatt zur Verfügung stehen.

Das Navigationssystem erleichtert die Fahrt zu unbekannten Zielen ebenso wie das Umfahren von Staus, doch sein Bewegungsprofil will der Fahrer nicht ohne seine Zustimmung im Internet veröffentlicht sehen. Vergleichbares gilt für die Datenübermittlung an jene Services, mit denen die Kfz-Versicherungen künftig im Wettbewerb um die günstigsten Tarife punkten wollen.

Für das Connected Car ist damit eine Ende-zu-Ende-Sicherheitsarchitektur erforderlich. Anhand einer Konzeptstudie im Rahmen der **"Cape to Cape Challenge 2014"**[5] - des jüngsten Rekordversuchs von Rekordjäger Rainer Zietlow - hat HP aufgezeigt, welche Komponenten im Rahmen eines solchen "End-to-End"-Sicherheitsansatzes betrachtet werden können.

IT-Sicherheit in Extremsituationen

Die IT des Touareg-Teams musste nicht nur kontinuierlich aktuelle Daten übermitteln, sondern zugleich strengste Sicherheitsvorgaben einhalten. Für durchgängige, mehrschichtige IT-Sicherheit beim Rekordversuch sorgten Hardware, Software und Services von HP.



Rainer Zietlows Team hatte zwei HP Slate Tablets an Bord: eines für die Navigationssoftware, das andere für eine von HP entwickelte Daten-Logging-Applikation.
Foto: HP Deutschland

Die Konzeptstudie setzte schon bei den Endgeräten an. Zietlows Mannschaft nutzte HP Slate Tablets, die auf Android basieren und von HP abgesichert wurden. Mit diesen Geräten und einer von HP entwickelten App wurden die verschlüsselten Fahrzeugdaten per Bluetooth-Dongle ausgelesen und in einen verschlüsselten lokalen Container des Tablets überspielt.

Die Cloud-basierte Enterprise-Mobility-Management-Lösung HP Helion Mobility sorgte dabei für die zentrale Verwaltung der mobilen Geräte und Apps (Mobile Device Management, Mobile Application Management). Zugriffsmöglichkeiten auf Daten sowie App-Konfigurationen waren dank Helion Mobility über Richtlinien vorgegeben, bei einem Geräteverlust hätte man die Tablets zudem aus der Ferne löschen können.

Wie bereits skizziert, ist eine App erforderlich, um Daten aus dem Fahrzeug auszulesen und weiterzuleiten. Die Sicherheit dieser App nimmt dabei einen sehr hohen Stellenwert ein, insbesondere vor dem Hintergrund, dass laut einer Gartner-Studie heute - und auf absehbare Zeit - 75 Prozent der Mobilgeräte-Apps nicht einmal **grundlegende Security-Tests bestehen**[6]. Die Sicherheit bei der Programmierung mobiler Apps muss daher ein integraler Bestandteil jedes Connected-Car-Security-Konzepts sein.

So nutzt HP zum Beispiel bei der Programmierung von Apps bewährte App-Frameworks wie MSDLC (Microsoft Secure Development Lifecycle). Die Application-Security-Lösung HP Fortify wiederum stellt sicher, dass die Anwendungsentwicklung hohen Sicherheitsstandards entspricht. Fortify dient hier der Code-Analyse mobiler Apps im Hinblick auf Programmierfehler und Schwachstellen. Unter dem Namen "HP Fortify on Demand" steht die Lösung Anwendungsentwicklern als Cloud-Dienst auf Abruf zur Verfügung.

Sobald bei Zietlows Fahrt eine Mobilfunkverbindung vorhanden war, leitete die App die Daten verschlüsselt zur Auswertung an die HP Helion Cloud weiter, woraufhin die App die lokal zwischengespeicherten Daten automatisch löschte. Auf diese Weise bestand von den Datenloggern über die Slate Tablets bis zur Helion Cloud eine durchgehende Verschlüsselungskette. Eine solche lückenlose Absicherung des Datenverkehrs ist im Connected-Car-Umfeld unerlässlich, geht es doch um sensible Daten, die teils - sofern sie den Fahrer betreffen - auch dem Datenschutzgesetz unterliegen.

Sicherheit in der Cloud

Am anderen Ende der Verschlüsselungskette dürfen auch die Cloud-Rechenzentren keine Schwachstelle im Sicherheitskonzept darstellen. Die Helion-Rechenzentren nutzen deshalb HPs Server und Firewalls sowie die Netzwerksicherheitslösungen der Produktfamilie TippingPoint zum Aufspüren verdächtigen Datenverkehrs. Des Weiteren sind die HP Rechenzentren nach ISO 27001 zertifiziert und werden jährlich auditiert.

Eine wesentliches Sicherheitsproblem besteht laut einer **Studie des Ponemon Institute**[7] darin, dass es durchschnittlich 240 Tage dauern kann, bis eine IT-Organisation einen getarnten Angriff erkennt und somit in der Lage ist, darauf zu reagieren. Um die Response-Zeit im Angriffsfall zu minimieren, nutzt HP seine eigene SIEM-Lösung (Security Information and Event Management) namens HPArcSight. Sie bietet hochentwickelte Sicherheitsanalysen zur Identifikation von Bedrohungen und damit zurEingrenzung von Risiken, damit ein Unternehmen bestmöglich geschützt ist.

Um Unternehmen bei der Umsetzung durchgängiger Sicherheitskonzepte zu unterstützen, verfügt HP weltweit über mehr als 5.000 Sicherheitsfachleute, die die Kunden mit ihrem Know-how bei Projekten wie zum Beispiel der sicheren Anbindung von Fahrzeugflotten unterstützen. HP errichtet derzeit in Böblingen ein Security Operations Center (SOC), um die Nachfrage deutscher Kunden aus unterschiedlichen Branchen, darunter neben dem Automobilbau zum Beispiel auch die Finanzindustrie, direkt vor Ort bedienen zu können.

Die Vernetzung des Automobils schreitet zügig voran und ist dank zahlreicher Vorteile nicht mehr aufzuhalten. Doch dies birgt auch Risiken, denen man mit einem gesamtheitlichen Sicherheitskonzept begegnen muss, das vom Bordcomputer des Autos über Fahrzeug-Apps bis zu Cloud-Services reicht. Bei der Cape to Cape Challenge 2014 hat HP demonstriert, wie solch ein Gesamtkonzept aussieht und wie es funktioniert. Ganzheitliche Sicherheitskonzepte für vernetzte Autos müssen Alltag werden, denn mit dem Connected Car fließen IT-Sicherheit und Verkehrssicherheit zusammen.

Links im Artikel:

[1] **https://www.computerwoche.de/a/audi-demonstriert-pilotiertes-parken,2530604**
[2] **http://www.extremetech.com/extreme/181508-googles-self-driving-car-passes-700000-accident-free-miles-can-now-avoid-cyclists-stop-for-trains**
[3] **http://www.nytimes.com/2014/05/28/technology/googles-next-phase-in-driverless-cars-no-brakes-or-steering-wheel.html**
[4] **https://www.blackhat.com/us-14/briefings.html#a-survey-of-remote-automotive-attack-surfaces**
[5] **https://www.cio.de/brandlog/bvex_log/2971201/**
[6] **https://www.gartner.com/newsroom/id/2846017**
[7] **http://www8.hp.com/hpnext/posts/2014-cost-cyber-crime-study-reveals-increased-risks**