Security im vernetzten Fahrzeug

Intelligente Automobile sind nicht zwangsläufig sicher. Wie jedes internetfähige Gerät können auch sie zum Ziel von Cyberangriffen werden. Diese neue Fahrzeuggeneration bietet durch die mobilen Services eine wesentlich breitere Angriffsfläche als herkömmliche Automobile. Die Automobilbranche steht daher vor großen Herausforderungen, denn das Thema ist ebenso brisant wie komplex.

Erst kürzlich beschrieb ein Artikel in der amerikanischen Zeitschrift Forbes, wie Hacker in der Lage sind, die Kontrolle über ein von einer anderen Person gesteuertes Fahrzeug zu übernehmen. Die Konsequenzen derartiger Übergriffe könnten verheerend sein. Was würde passieren, wenn ein Hacker ein Fahrzeug per Fernsteuerung entriegeln oder den Motor während der Fahrt ausschalten würde? Ebenso vorstellbar sind Hackerangriffe, bei denen die persönlichen Daten des Fahrers in die falschen Hände geraten.

Persönliche Daten

Vernetzte Fahrzeuge speichern in großem Umfang persönliche Daten. In vielen Fällen ist strittig, wem diese Daten gehören – dem Fahrer oder dem Hersteller? Ein Beispiel: Vernetzte Automobile sind mit dem Fahrverhalten des Fahrers vertraut. Wird das Fahrzeug „ausplaudern", dass er regelmäßig die Höchstgeschwindigkeit überschreitet oder während der Fahrt Textnachrichten schreibt? Werden ihm günstigere Versicherungstarife angeboten, wenn er sicherheitsbewusst fährt? Aus Gründen der Verkehrssicherheit sollte das Auto unter bestimmten Umständen die Polizei informieren. Aber wird dadurch nicht die Privatsphäre verletzt? Daten zu Wartungszwecken und Serviceleistungen gehören zweifellos dem Hersteller. Doch wie verhält es sich mit dem Rest der erfassten Daten?

Diese Frage kann nicht eindeutig beantwortet werden. Gegenwärtige Datenschutzrichtlinien weisen noch Lücken auf. Finden vernetzte Fahrzeuge eine größere Verbreitung, wird dieses komplexe Thema weitere Beachtung finden. So sind derzeit nicht einmal die Datenschutzregeln innerhalb Europas einheitlich, was die Nutzung der mobilen Services schon durch einen Grenzübergang erschwert. Das Thema ist ebenso brisant wie komplex. Die öffentliche Diskussion steht hier noch ganz am Anfang.

Die Automobilbranche steht vor großen Herausforderungen, wenn diese Bedrohungen effektiv abgewehrt werden sollen. Bereits jetzt sollten dem Datenzugriff und der Datensicherheit bei der Herstellung vernetzter Automobile höchste Priorität eingeräumt werden. Die durchdachte Nutzung von APIs (Application Programming Interface) zur Verbindung von Fahrzeugen mit dem Internet hilft Automobilherstellern, diese Herausforderungen zu bewältigen und sich auf dem Markt zu behaupten.

Schnittstellen sind der Schlüssel

Im Hinblick auf zukünftige Entwicklungen in der Fahrzeuginteraktion kommen APIs eine besondere Bedeutung zu. APIs, oder genauer gesagt REST3 APIs, spielen eine zentrale Rolle bei der Verbindung von Geräten mit dem Internet. Ein API kann man sich als Boten zwischen App und Gerät vorstellen. In diesem speziellen Fall ist das vernetzte Automobil das Gerät. Diese Schnittstelle ermöglicht beispielsweise die Registrierung von Entwicklern und Apps, die Verteilung und den Widerruf von API-Schlüsseln sowie die API-Versionsverwaltung. Die Schnittstellen müssen jedoch unbedingt verwaltet werden: Ohne ein effektives API-Management können die APIs eines Automobilherstellers von Schadcode infiziert oder angegriffen werden. Wenn ein Hacker sich Zugriff zu einem API verschafft, ist er unter Umständen in der Lage, unbefugt die Kontrolle über ein Fahrzeug zu erlangen.

Denn APIs erfüllen entscheidende Aufgaben: Zum einen vernetzen sie das Fahrzeug mit dem Server, ganz egal, ob dieser sich in einem klassischen Rechenzentrum oder in der Cloud befindet. So erhält der Hersteller Zugang zu den Servicedaten und anderen Kennzahlen. Zum anderen verschaffen sie dem Fahrer Zugang zu seinem Wagen und seinen mobilen Services. Dabei muss beispielsweise die Identität des Fahrers zweifelsfrei überprüft werden können und ein persönliches Profil hinterlegt sein. Für einen Automobilhersteller mit hunderttausenden Kunden ist allein dieses Identitätsmanagement eine gewaltige Aufgabe. Heutige API-Sicherheitsmethoden bieten jedoch verlässliche Wege, solche API-Infrastrukturen umzusetzen. Zudem existieren bereits leistungsfähige Sicherheitsstandards im API-Umfeld, wie etwa der ursprünglich für die sichere Autorisierung von Internetanwendern entwickelte OAuth 2.0-Standard, der für Identity Federation genutzt wird. Diese Spezifikationen und Erfahrungen können Automobilhersteller nutzen.

i Über Axway

Axway ist ein international agierender Softwarehersteller mit mehr als 11.000 Kunden in 100 Ländern. Seit mehr als einem Jahrzehnt unterstützt Axway weltweit führende Unternehmen aus dem öffentlichen und privatwirtschaftlichen Sektor. Die Lösungen für das Management geschäftskritischer Interaktionen regeln die Datenflüsse im Unternehmen, zwischen B2B-Communities sowie in Cloud- und mobilen Anwendungen. Das Portfolio reicht dabei von Business-to-Business-Integration und Managed File Transfer über API- und Identitätsmanagement bis hin zu E-Mail-Sicherheit. Das Angebot erfolgt On-Premise oder in der Cloud mit Professional und Managed Services.
Axway ist in Frankreich registriert und unterhält neben dem Hauptsitz in den Vereinigten Staaten Niederlassungen in 19 Ländern.

Das Auto der Zukunft

Moderne Fahrzeugtechnologie entwickelt sich in einem atemberaubenden Tempo. Deshalb ist es nicht unwahrscheinlich, dass sich das Automobil zum ultimativen Mobilgerät der Zukunft aufschwingt. Bereits jetzt betrachten Autohersteller Fahrzeuge als mobile Unterhaltungsplattformen. Um jedoch erfolgreich ein neues mobiles Zeitalter einzuläuten, müssen sich Autohersteller der potenziellen Gefahren des vernetzten Automobils bewusst sein und Maßnahmen ergreifen, um ihre Fahrzeuge zukunftssicher zu machen. Die Implementierung einer erfolgreichen API-Managementstrategie sollte dabei an erster Stelle stehen, um die virtuelle Sicherheit des Autos der Zukunft zu gewährleisten. ■ (oe)

» **www.axway.de**

Dietmar Koch ist VP Product Management, B2B/Automotive & eInvoice bei Axway.