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.

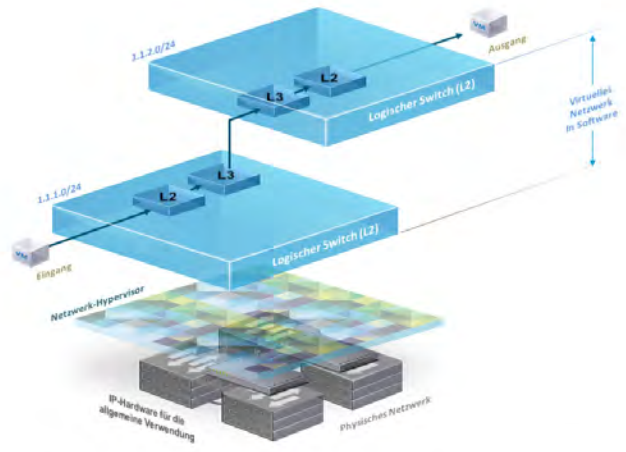
In diesem Zusammenhang ist ein wichtigstes Element für ein persönlicheres und vernetztes Erlebnis im Fahrzeug durch Apps oder Services die Garantie, dass die betroffenen persönlichen Daten privat bleiben. Gleichzeitig müssen auch Hersteller ihre eigenen Infrastrukturen und Daten vor Angriffen gegen Kunden 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.