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