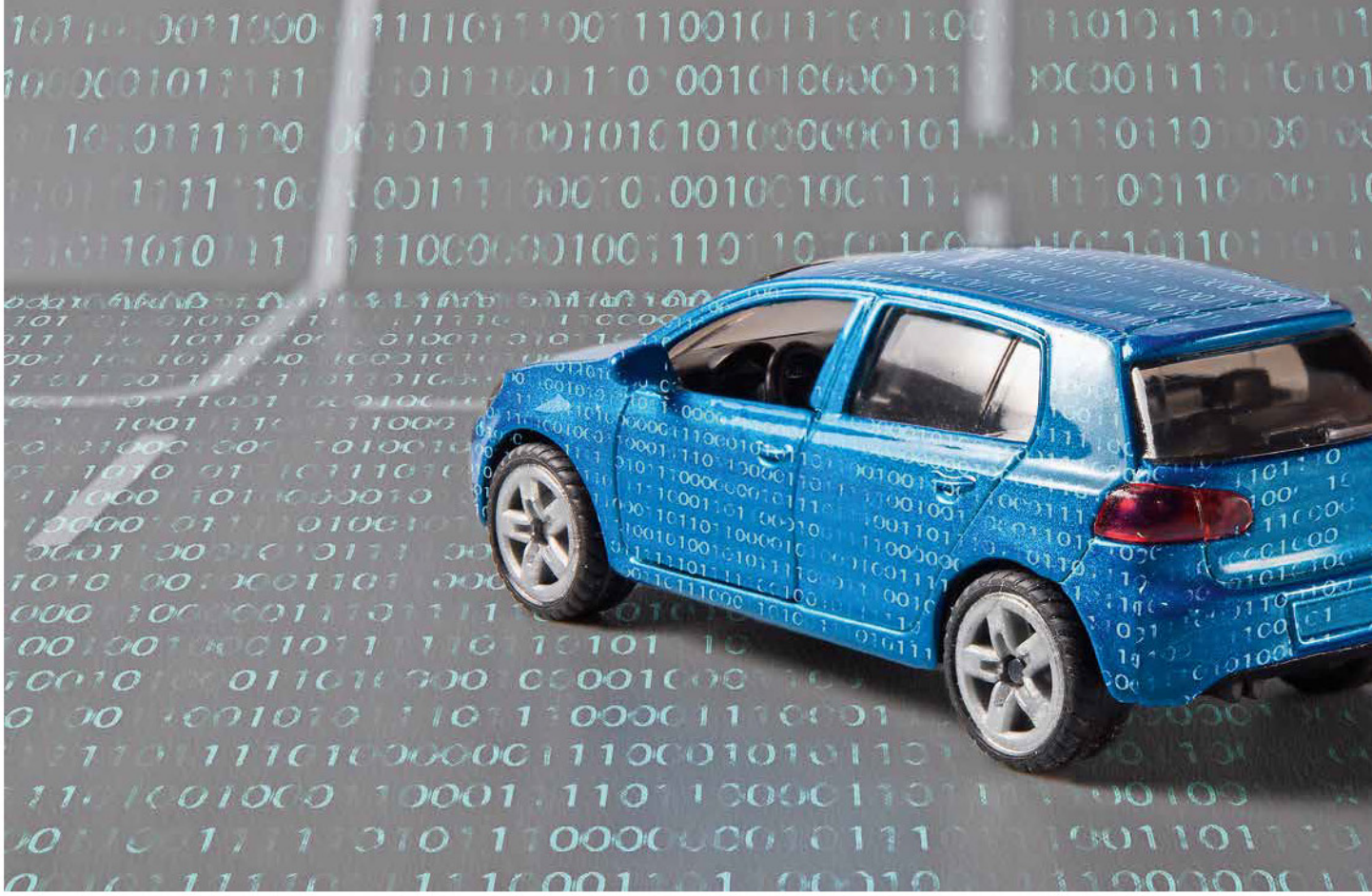

# Rollende Datenbanken

In aktuellen Fahrzeugmodellen verbauen die Hersteller 60 bis 80 Computer. Sie sind untereinander und mit der Außenwelt vernetzt. Und die Anzahl sowie der Vernetzungsgrad werden künftig nicht geringer.

**HOLGER PINNOW-LOCNIKAR**

Im Internet of Things (IoT) sollen die Autos in naher Zukunft nicht nur miteinander, sondern auch mit Verkehrsampeln, anderen motorisierten Verkehrsteilnehmern und diversen Verkehrsleit- und Überwachungssystemen kommunizieren – von den enormen Anforderungen des angestrebten autonomen Fahrens mal ganz abgesehen. IoT-Visionäre sehen die Autos auch schon mit dem heimischen Garagentor oder der Kaffeemaschine parlieren.

All diese Zukunftspläne und -visionen stellen die Hersteller vor gewaltige Herausforderungen, besonders was die Sicherheit der hochkomplexen Systeme betrifft. So muss der Produzent eines Autos nicht nur sicherstellen können, dass die intelligenten Fahrzeugsteuerungs- und Sicherheitssysteme unter allen Umständen fehlerfrei funktionieren und damit kein Risiko für die Fahrer, Insassen und andere Verkehrsteilnehmer erzeugen, er ist auch verantwortlich für die Security des Autos über seine gesamte Lebensdauer – also die Sicherheit gegenüber Hackern.

Ein Securityspezialist ist Prof. Dr. Jörn Eichler, der das Thema Security Engineering bei Volkswagen Pkw in der Technischen Entwicklung verantwortet und die Arbeitsgruppe Secure Systems Engineering am Institut für Informatik der FU Berlin leitet. Eines der primären Ziele der Hersteller ist eben dieser Schutz der Systeme vor unbefugtem Zugriff und Manipulation: „Der Hersteller muss sich in die Position des Hackers hineinversetzen, um Bedrohungen zu antizipieren", beschreibt Eichler die Vorgehensweise. Entsprechend ergreift der Hersteller Maßnahmen zur Risikobegrenzung. Problem: Auch die Angreifer lernen dazu. Der Hersteller muss dann auf die Veränderung der Bedrohungslage reagieren können. Die Hersteller stehen damit vor großen Aufgaben: „Je stärker Systeme auch über die Fahrzeuggrenze hinaus vernetzt werden, desto größer wird die Angriffsoberfläche", unterstreicht Eichler.

> „Der Hersteller muss sich in die Position des Hackers hineinversetzen, um Bedrohungen zu antizipieren."
>
> **Prof. Dr. Jörn Eichler,** Securityspezialist bei Volkswagen Pkw

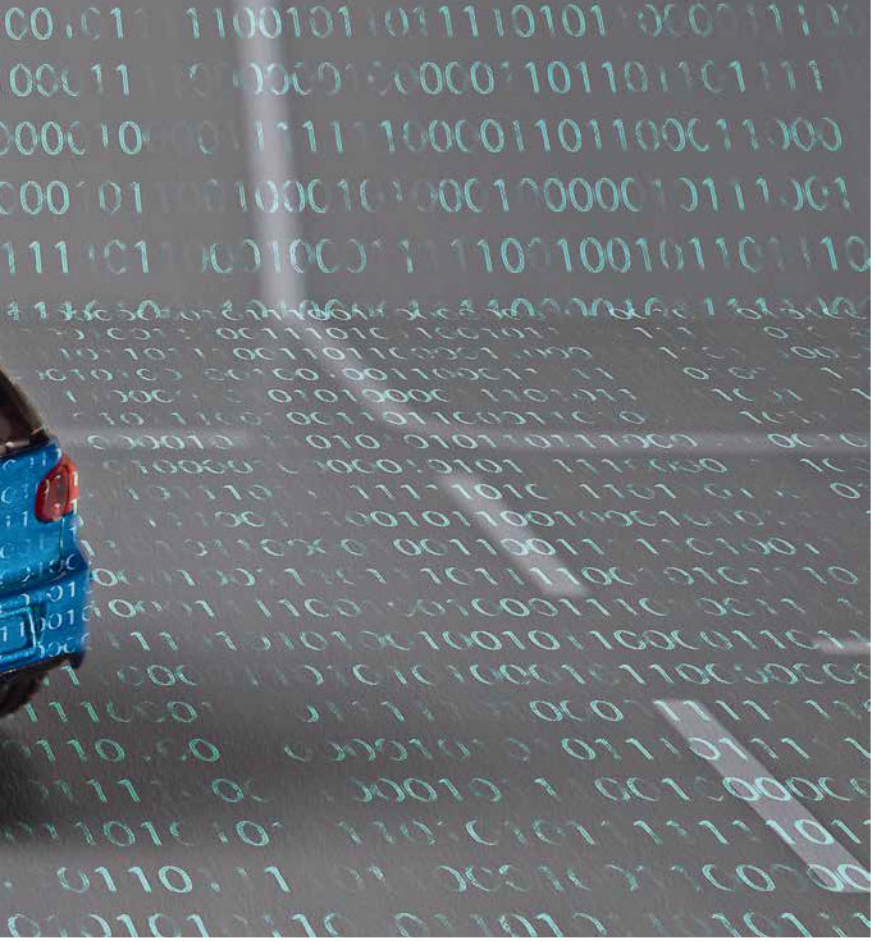

Foto: Uli-B - Fotolia.com

„Automatisierte Fahrfunktionen erhöhen dabei das Schadenspotenzial."

Die juristische Grundsatzposition – der Hersteller bleibt über die gesamte Lebensdauer des Fahrzeugs für dessen Sicherheit verantwortlich – macht es den Entwicklern nicht einfacher. Aber man wähnt sich auf einem guten Weg: „Verbesserte Systemleistungen ermöglichen zusätzliche Schutzmaßnahmen." Dabei müssen die Entwickler auch neue Wege gehen, um den Hackern immer einen Schritt voraus zu sein: „Herkömmliche Implementierungen drahtloser Technologien wie WLAN oder Bluetooth sind auch den Angreifern hinlänglich bekannt." Technisch bereiten sich die Hersteller auf 5G und V2X vor, mit Narrowband IoT als Zwischenlösung. Darüber hinaus sind Standards bisher allerdings Mangelware: Die europäischen Autobauer forschen jeder für sich und keiner will sich in die Karten schauen lassen.

Die Datensicherheit ist aber nicht nur eine Frage der Abwehr äußerer Angreifer. Die DSGVO regelt den Datenschutz auch für Verkehrsteilnehmer. Diese haben ein Recht darauf, über die in Zusammenhang mit ihrer Mobilität übermittelten und gespeicherten Daten Bescheid zu wissen und diese gegebenenfalls löschen zu lassen oder deren Weitergabe freigeben oder untersagen zu dürfen. Über die verbindliche Einhaltung der Regeln wacht die Europäische Datenschutzkommission. Volkswagen entwickelt eine umfassende digitale Kundenakte unter dem Namen Volkswagen-ID, über die vom Kauf des Autos inklusive Zahlungsabwicklung über Wartung, Service und Reparatur bis hin zur Stromabrechnung an Ladesäulen und Over-the-Air-Updates alles abgewickelt werden soll. Diese Pläne werfen viele Fragen auf, da es hier nicht nur um technische, sondern vor allem um personenbezogene Daten geht – Fragen nach der Datensicherheit und nach der Datenverfügbarkeit für den Fahrzeughersteller und sein Wartungspersonal, aber auch für Serviceleistungen aus der Hand freier Anbieter.

Das Sammeln von Fahrzeugdaten ist für die Hersteller von herausragender Bedeutung. Dabei geht es in erster Linie um die Überwachung und Wartung der Fahrzeugsysteme. Entsprechend bereitet den Herstellern die Tatsache, dass ihre Fahrzeuge irgendwann nach Ablauf der Garantiezeiträume auch von Dritten gewartet werden könnten, Kopfzerbrechen. Jens Bobsien, Pressesprecher der Volkswagen AG, räumt ein, dass die Wartung von Securitysystemen oder sicherheitstechnisch geschützten Systemen es allein aus technischen Gründen erforderlich machen könnte, den Zugriff nur berechtigtem Wartungspersonal unter Verwendung von Spezialwerkzeug zu gestatten. Anders sei es nicht möglich, Systeme und Bauteile gegen Manipulation zu schützen. Man muss kein Prophet sein, um die Problematik für den freien Ersatzteilmarkt und die freien Werkstätten zu erkennen.

Weitere Fragen müssen noch auf Antworten warten: Muss der Kunde mit einer Volkswagen-ID Nachteile befürchten, wenn er eine freie Werkstatt aufsucht? Welche Daten aus der digitalen Kundenakte können freie Werkstätten beim Service einsehen – und wer hat die Rechte an den Daten? Bobsien versichert, dass die VW-ID und die dafür benötigten Systeme nach dem neuesten Stand der Datensicherheitstechnik entwickelt werden. Aber ansonsten hält sich Volkswagen hier im Moment noch bedeckt – vielleicht auch, weil es noch nicht auf alle Fragen Antworten gibt. ■

Foto/Montage: Volkswagen/Holger Pinnow-Locnikar

Prof. Dr. Jörn Eichler leitet die technische Entwicklung des Security Engineering bei Volkswagen Pkw.