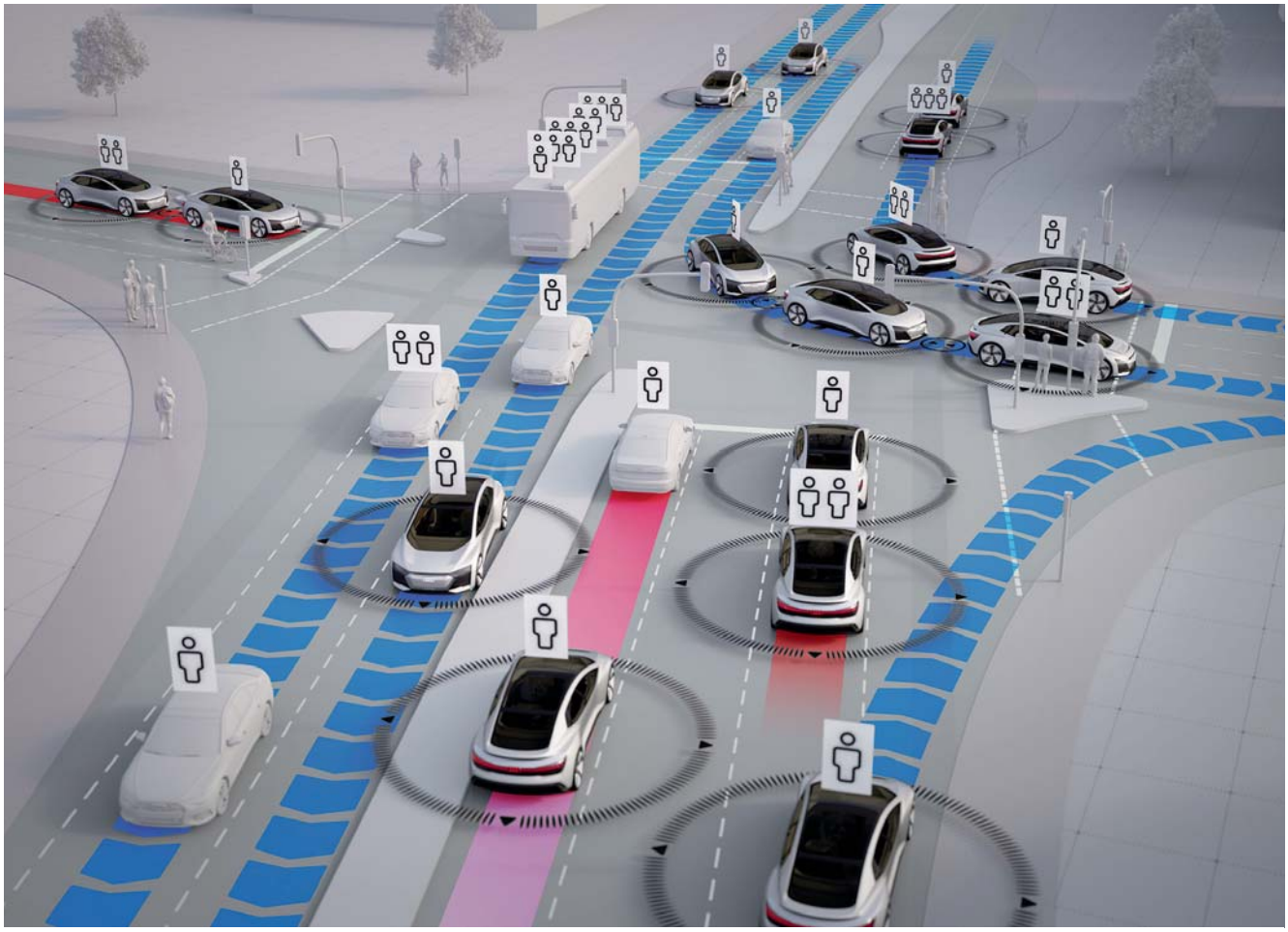
Gefährliche Lücken

Pkw sind rollende Computer. Mit der Verwandlung zu einem internetfähigen Hightechgefährt gehen die IT-typischen Gefahren einher. Gerade bei vernetzten Autos wird Cybersecurity immer wichtiger.

Moderne Autos sind rollende Computer und als solche können sich auch unerwünschte Besucher Eintritt in die Systeme verschaffen und das Fahrzeug kapern. Die Gefahr ist nichts Neues: Vor rund sechs Jahren nutzten zwei Hacker eine Sicherheitspforte im Infotainment von einem Jeep Cherokee und übernahmen die Steuerung der Bremsen sowie der Lenkung. Der Imageschaden für Fiat Chrysler war immens und 1,4 Millionen Fahrzeuge mussten in die Werkstätten zurückgerufen werden, um die Sicherheitslücke zu schließen. Wie bei jedem modernen PC gibt es sicher bei einem Pkw nicht nur eine Sicherheitslücke. Klar ist auch, dass jedes moderne Auto mit autonomen Fahrfunktionen, wie einem adaptiven Tempomaten oder einem Spurhalteassistenten inklusive Lenkeingriff, von Hackern in ein „Zombie-Fahrzeug" verwandelt werden kann. „Für mich gibt es keine unkritischen Daten im Zusammenhang mit dem Auto als Verkehrssystem", verdeutlicht es Udo Schneider von Trend Micro, einem global agierenden Cybersecurity-Unternehmen.

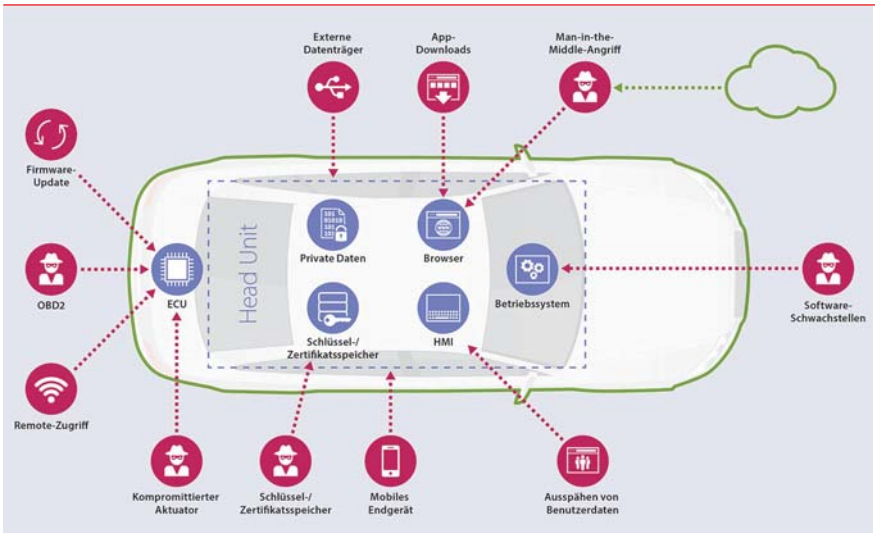
Was ist mit Google Maps?

Viele Autofahrer nutzen Kartendienste wie Google Maps. Auch bei Flottenbetreibern setzt sich diese Art des günstigen Navigierens durch, zumal der US-Hightechkonzern jetzt auch CO_2-optimierte Routen anbietet. Google Maps bekommt somit eine Funktion, die den Kartendienst zum ökolo-



Fotos: Escrypt/Rocco Swantusch/Autoflotte

Ohne Vernetzung aller Verkehrsteilnehmer miteinander und mit der Umgebung wird es in Zukunft nicht mehr funktionieren



Angriffspunkte für Hacker gibt es im modernen Automobil viele. Autohersteller, Softwareanbieter sowie Zulieferer im Hardware-Bereich und auch Telekommunikationsunternehmen müssen eng miteinander arbeiten

gischen Schweizer Armeemesser macht. Denn die beliebte Navigations-App wählt in Zukunft standardmäßig die Route aus, auf der am wenigsten CO_2-Ausstoß generiert wird. „Wir gehen davon aus, dass wir für etwa die Hälfte der Routen eine umweltfreundlichere Option mit minimalem oder gar keinem Zeit-Kosten-Kompromiss finden können", erläutert Google Produkt-Direktor Russell Dicker.

Doch bei Google gilt seit jeher das Prinzip: Auch wenn man nichts dafür bezahlen muss, ist es noch lange nicht umsonst. Daten sind ein lohnendes Geschäft. Der Gigant aus dem Silicon Valley nutzt unter anderem die Bewegungsdaten, um seine Navigations-App zu betreiben. Das ist mittlerweile „business as usual". Die CO_2-Routen sind eine ganz andere Hausnummer. Um die Emissionsbilanz einer Fahrt zuverlässig voraussagen zu können, ist eine Vielzahl von Parametern nötig, die in komplexe Berechnungen einfließen. Unter anderem die Topografie der Straßen, die vermutete Geschwindigkeit des Fahrzeugs und natürlich die Motorisierung samt Abgasnorm.

Laut Google werden die Emissionen des Wagens anhand der Ergebnisse durch Tests verschiedener Fahrzeug- und Straßentypen kalkuliert. Die Daten zur jeweiligen Straßenqualität stammen von den Street-View-Autos sowie von Luft- und Satellitenbildern. „Google wertet eine Vielzahl verschiedener Datenquellen aus. Dass hier kritische Daten ermittelt oder verarbeitet werden, sehe ich nicht", gibt Jan Becker von Apex.AI, die autonome Fahrsysteme entwickeln, Entwarnung.

Großer Bruder fährt bereits mit

Neben Google interessiert sich auch die EU für die Verbrauchsdaten der Automobile. Seit letztem Jahr müssen die Automobilhersteller die Realverbräuche der Neuwagen nach Brüssel senden. Das erkennt man auch an der aktuellen Abgasnorm Euro 6d-ISC-FCM, wobei die Buchstaben „FCM" für „Fuel Consumption Monitoring" stehen. Also fährt der „Große Bruder" mit dem gelben Sternenkreis auf der blauen Fahne bei jedem Kilometer mit. Um den Verbrauch zu ermitteln, ist ein Standard-Messgerät namens „On-Board Fuel Consumption Meter" (OBFCM) installiert. Überwacht werden neben dem Kraftstoff- beziehungsweise dem Stromverbrauch auch Fahrgeschwindigkeit und Laufleistung. Diese Daten zeichnet jeder moderne Pkw ohnehin auf. Audi nutzt bei Fahrzeugen wie dem neuen A3 die Generic-Scan-Tool-Schnittstelle, um die Werte gemäß dem Industriestandard ISO 15031-5 zu übertragen beziehungsweise per Diagnose-Tester bei einer Inspektion auszulesen. Auch hier beruhigt Jan Becker: „Die EU ist an den Flotten- und Modellverbräuchen interessiert, nicht an denen einzelner Individuen, ich würde daher nicht vom gläsernen Fahrer sprechen."

Steffen Krautwasser, Flottenchef bei SAP, widerspricht: „Jegliche zusätzliche Übertragung und Speicherung ist ein zusätzliches Einfallstor und ein zusätzliches Risiko. Wichtig in diesem Zusammenhang wäre aus meiner Sicht die Anonymisierung der Daten. Es ist für mich nicht ersichtlich, wozu die Fahrgestellnummern übertragen werden müssen. Zur ‚Kontrolle' oder besser formuliert Auswertung der Daten würden Hersteller, Modell, Motorvariante, Baujahr ausreichen. Eine Eins-zu-eins-Zuordnung ist in diesem Bereich nicht notwendig, da es keine zusätzlichen Vorteile bringt."

NFC-Chips

Die Einfallsschleusen zu einem Automobil sind mannigfaltig. Neben der bereits erwähnten OBD-Schnittstelle bieten Smartphones, die zugleich als Autoschlüssel oder Ladesäulenfreischaltung genutzt werden, eine Angriffsfläche, um in die Software der Autos einzudringen. Beim Handy-Autoschlüssel wird eine App sowie der NFC-Chip des Smartphones genutzt, um sich Zugang zum Auto zu verschaffen. Um die Daten des virtuellen Schlüssels möglichst sicher zu verwahren, sind sie wie die Kreditkartendaten auf dem „Secure Element" des NFC-Chips abgespeichert. „Der Schlüssel darf nicht kopierbar sein, und wir brauchen im Falle eines Totaldiebstahls einen transparenten Überblick, wer wann für welchen Schlüssel berechtigt wurde", stellt Jochen Haug, Schadenvorstand Allianz Versicherungs-AG klar.

Grundsätzlich gilt das Betriebssystem der Apple-Handys als sicherer als das der Android-Telefone, da Apple ein geschlossenes System hat. Das ändert nichts an der Tatsache, dass sowohl die Automobilhersteller als auch die Smartphone-Hersteller gefragt sind, um das System wasserdicht zu machen. Diese Cyber-Sicherheit ist vor allem für Flottenbetreiber ein zentraler Punkt. „Generell sehe ich die Verwendung

Steffen Krautwasser, SAP, auf dem Autoflotte Fuhrparktag im Herbst 2019

„Aus meiner Sicht ‚gehören' die Daten teilweise den Fahrerinnen und Fahrern sowie dem Eigentümer, aber nicht dem OEM."

Steffen Krautwasser, Head of Global Car Fleet SAP

und Speicherung der Daten als kritisch an. Den Fahrerinnen und Fahrern ist bisher kaum bekannt, welche Daten überhaupt und für wie lange gespeichert werden. Hier ist mehr Transparenz notwendig. Das Gleiche gilt auch für mich als Flottenmanager. Transparenz, Einsicht und Löschung der Daten sollten jederzeit möglich sein. Aus meiner Sicht ‚gehören' die Daten teilweise den Fahrerinnen und Fahrern sowie dem Eigentümer, aber nicht dem OEM", sagt Steffen Krautwasser. Der Flottenmanager sieht aber auch Vorteile bei der Wartung, indem zum Beispiel Defekte früh erkannt werden und dadurch Kosten gespart werden können.

Stichwort Car2Car

Schaut man in die Zukunft, wird die Cybersecurity durch die vernetzten Fahrzeuge – Stichwort Car2Car und Car2X (Kommunikation zwischen Fahrzeug und Umwelt) – noch deutlich relevanter, als es ohnehin schon ist. Damit wird die Aufgabe für die Hersteller nicht einfacher. Zumal die Autos im Zuge der Automatisierung immer komplexer werden und eine umfangreichere Software benötigen. Bei Automobilen gilt der gleiche Grundsatz wie bei den heimischen Computern, dass man die Systeme und die Software immer möglichst aktuell halten soll. Viele Aktualisierungen – vor allem für das Infotainment – laufen drahtlos ab. Künftig sollen Over-the-Air auf Wunsch auch weitere Funktionen des Autos freigeschaltet werden. Wieder eine Möglichkeit für Hacker, sich Zutritt zu den Systemen des Vehikels zu verschaffen.

Das erkennt auch die UN und ergreift Maßnahmen, um der Bedrohung Herr zu werden. Das „UNECE World Forum for Harmonization of Vehicle Regulations" hat bereits im vergangenen Jahr einige neue Regelwerke zu Cybersicherheit und Software-Updates von vernetzten Fahrzeugen verabschiedet. Folgende Vorschriften gelten für Pkw, Transporter, Lkw und Busse:

- Security-by-Design bei der Fahrzeugentwicklung, um Risiken entlang der Wertschöpfungskette zu mindern
- Bereitstellung sicherer Software-Updates und Einführung einer Rechtsgrundlage für Over-the-Air-Updates
- Management der Cyberrisiken für Autos
- Angriffserkennung und -abwehr für die gesamte Fahrzeugflotte

In der Europäischen Union wird die neue Verordnung ab Juli 2022 für alle neuen Fahrzeugtypen und ab Juli 2024 für alle ab diesem Zeitpunkt hergestellten Neufahrzeuge verpflichtend. „Aufgrund der neuen Regulierung muss daraus nun ein ganzheitlicher Ansatz geformt werden, welcher den kompletten Lebenszyklus eines Fahrzeugs umfasst", erklärt Sebastian Rist, Projektleiter und Security Consultant bei Escrypt, einem Unternehmen, das sich auf Sicherheitslösungen spezialisiert hat.

An der Hacker-Ehre gepackt

Um die Vorgaben konsequent umzusetzen, ist ein umfassendes „Cybersecurity Management Systems" (CSMS) nötig. Allerdings ist die Realisierung eines solchen Werkzeugs aufgrund der Komplexität des Automobils nicht ganz einfach. Das geht bereits in der Produktion und der Lieferkette los. Schließlich versorgen die Zulieferer die Autobauer mit den Modulen, die durchaus sicherheitsrelevant sind. Und wo Software ist, gibt es auch Einfallstüren.

Die Autobauer halten die IT-Karten daher nahe an der Brust. Laut einer Studie der Unternehmensberatung Capgemini bleiben Dateneigentum und Cybersicherheit kritische Punkte: Rund die Hälfte der OEMs hat damit zu kämpfen, Daten zu sammeln und daraus verwertbare Erkenntnisse abzuleiten. Weniger als zehn Prozent glauben, dass sie gut vorbereitet sind, Cybersicherheitsmaßnahmen umzusetzen und 60 Prozent haben Schwierigkeiten, sicherzustellen, dass die Produkte von Zulieferern den Sicherheits- und Cybersicherheitsvorschriften entsprechen.

Aus gutem Grund: Wer mit einem sicheren System prahlt, weckt den Ehrgeiz der Hacker. „Die höchsten Sicherheitsansprüche unserer Kunden gelten in gleicher Weise für die Datensicherheit des vernetzten Fahrzeugs als auch unserer Kundendaten. Daimler schützt die Kundendaten vor Manipulationen und Missbrauch. Mit Blick auf den IT-technischen Fortschritt entwickeln wir die Datensicherheit ständig weiter", lässt der schwäbische Premium-Autobauer verlauten. *Wolfgang Gomoll*

Neue Regulierungen bedingen einen ganzheitlichen Ansatz, meint Sebastian Rist, Security Consultant bei Escrypt