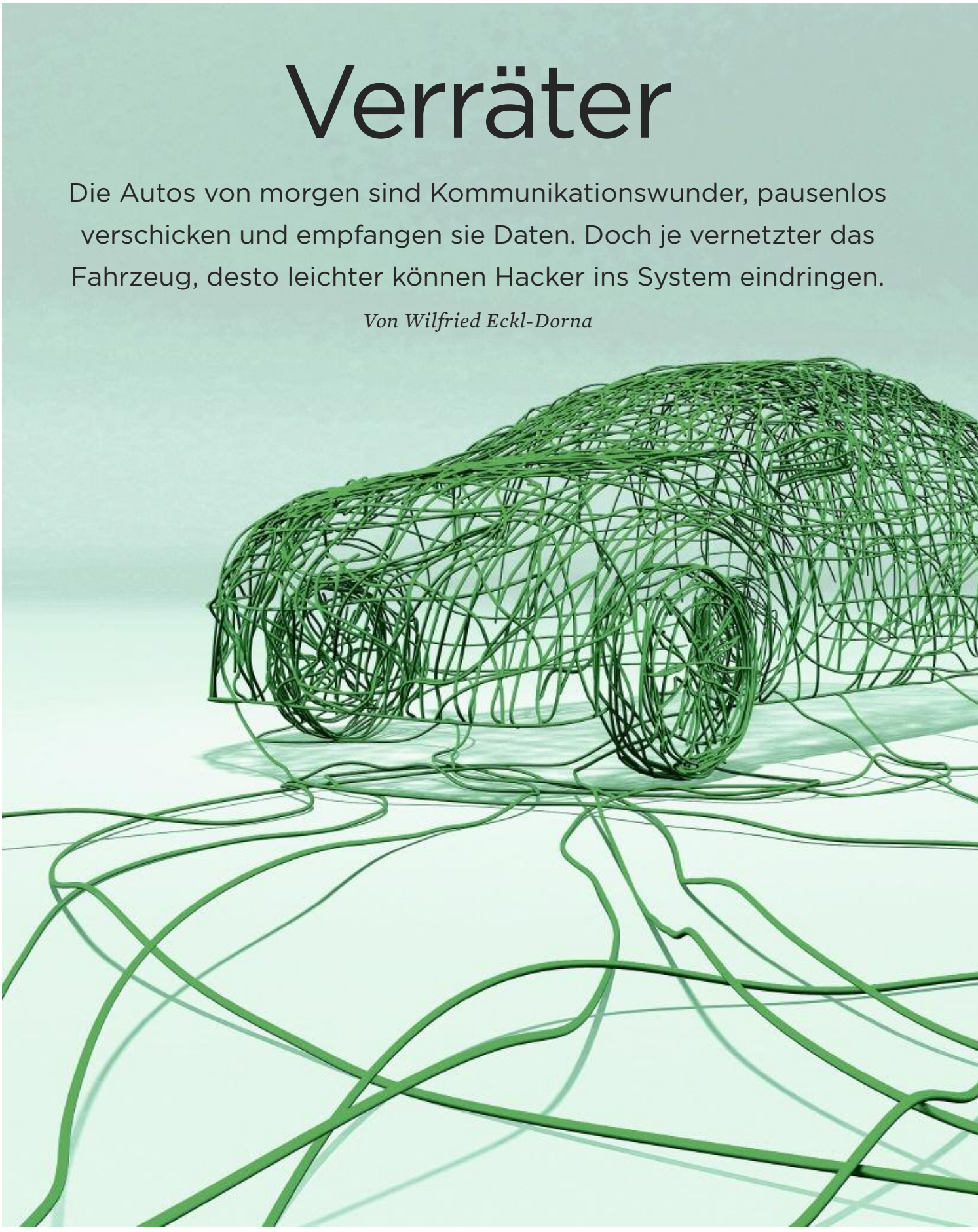
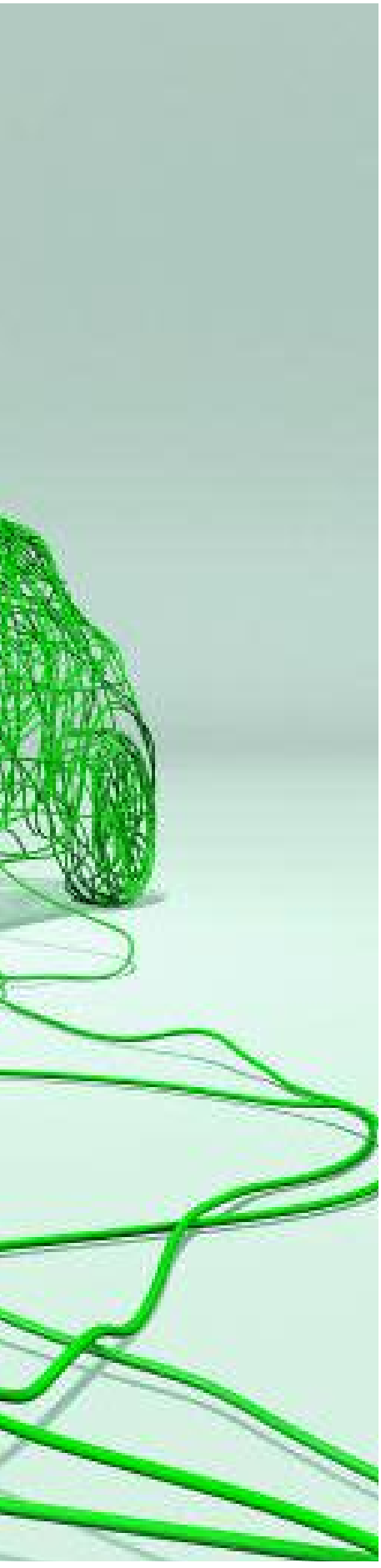
Verräter

Die Autos von morgen sind Kommunikationswunder, pausenlos verschicken und empfangen sie Daten. Doch je vernetzter das Fahrzeug, desto leichter können Hacker ins System eindringen.

Von Wilfried Eckl-Dorna



MIGUEL NAVARRO / GETTY IMAGES



AUTOHERSTELLER und Flottenbetreiber lieben das handtellergroße Gerät: Die Telematik-Box setzt bei Unfällen Notrufe ab, ein eingebautes GPS-Modul übermittelt die genaue Position. Per Mobilfunk hilft sie beim Diagnostizieren und Beheben von Elektronikproblemen im Auto oder beim Vermeiden von Staus.

Auch Thomas Enderle kennt die Vorteile des Geräts. Doch seine Aufgabe ist es, die Schwachstellen aufzuspüren – im Auftrag von Autoherstellern. Eine gute Woche lang hat sich der studierte Mathematiker dafür Zeit genommen. Er hat Fotos von den Prozessoren gemacht, um deren Anschlüsse genau zu betrachten. Aus dem Internet hat er sich Datenblätter zu ähnlichen Bauteilen heruntergeladen, zuletzt hat er die Spannung an Leiterbahnen vermessen.

Nach seinen Recherchen befestigte er hauchdünne Drähte an bestimmten Stellen der Platine. Schnell hatte er die richtigen Zugangspunkte gefunden und konnte den internen Zustand des Prozessors auslesen. Und nicht nur das. „Im Prinzip habe ich komplett die Kontrolle übernommen“, sagt er. Genau das ist der Albtraum jedes Autoherstellers. Um solche Szenarien zu verhindern, engagieren die Autohersteller Unternehmen wie Enderles Arbeitgeber Escrypt.

Das Tochterunternehmen des Autozulieferers Bosch hat sich auf die Sicherheit eingebetteter Systeme spezialisiert – und die Auftragslage ist gut. Denn die Branche steht vor einer heiklen Aufgabe. Für neue Assistenzsysteme packen die Hersteller immer mehr Computertechnik in ihre Fahrzeuge und verknüpfen sie im Wageninneren. Damit sich Smartphones auch im Auto komfortabel nutzen lassen, gibt es im Innenraum mehr Funkschnittstellen zur Bordelektronik. Mobilfunkmodule ermöglichen eine ständige Internetverbindung im fahrenden Auto. Doch je mehr Verbindungen ein Auto nach außen besitzt, desto mehr Angriffsfläche bietet es.

Wenn die Autohersteller dabei nicht sehr behutsam vorgehen, könnte ein Hacker im schlimmsten Fall vom Schreibtisch aus die komplette Kontrolle über ein fahrendes Fahrzeug übernehmen. Noch ist die Branche von diesem Horrorszenario jedoch weit entfernt, meint Enderle. „Meine Manipulationen waren nur mit physischem Zugriff auf die Hardware möglich. Dazu muss man schon Insider sein“, sagt er.

Allerdings sind Angreifern vereinzelt auch schon drahtlose Auto-Attacken geglückt. So gelang es chinesischen Studenten bei einem Hacker-Wettbewerb im Sommer dieses Jahres, das Schiebedach eines Tesla-Elektroautos per Funk zu öffnen und die Hupe zu betätigen – bei fahrendem Auto. Auch die Türen konnten sie aus der Ferne öffnen. An die Systeme für Bremsen oder Lenkung kamen sie aber nicht heran – anders als Forscher der Universität Washington und der University of California in San Diego, die im Jahr 2011 per Smartphone in die Elektronik eines Autos vordrangen und aus der Ferne die Bremse abschalteten.

Beide Attacken waren komplexe Vorgänge. Die chinesischen Studenten benötigten mehrere Tage, um die Kontrolle über Teile des Tesla Modell S zu übernehmen, mit einem Software-Update durch den Hersteller war das Problem schnell behoben. Die amerikanische Uni-Hackertruppe tüftelte noch deutlich länger: Monatelang analysierten zehn Forscher sämtliche Schwachstellen einer von ihnen nicht benannten Limousine. Am Ende funktionierten ihre Zugriffe auf die Bordelektronik nur bei dem von ihnen untersuchten Fahrzeug, weil die Hersteller für jedes Modell unterschiedliche Steuerungscodes verwenden.

DASS EIN ANGREIFER von seinem Schreibtisch aus die Bordelektronik fahrender Autos knackt, halten Experten deshalb für ausgeschlossen. „Autos aus der Ferne via Internet zu hacken ist noch unmöglich“, meint Enderles Chef Marko Wolf, Leiter der Münchner Escrypt-Niederlassung. Das wird auch noch länger so bleiben, glaubt er. Denn Autos seien für Hacker schwierige und vor allem teure Angriffsziele. Zwar läuft die Kommunikation zwischen den Steuergeräten in einem Auto-Bordnetz meist unverschlüsselt ab. Doch um die Steuerimpulse abzufangen, ist ein physischer Zugang zur Bordelektronik notwendig – also eine Kabelverbindung.

Wer die komplette interne Kommunikation eines Autos enträtseln will, braucht zudem viel Zeit. Er muss das Fahrzeug besitzen oder langfristig leihen, was einiges an finanziellen Ressourcen voraussetzt. In Neuwagen stecken heute bis zu 80 verschiedene elektronische Steuergeräte, die auch noch oft innerhalb einer Modellgeneration ausgetauscht werden. Die Steuerbefehle aus einem Automodell lassen sich deshalb nur schwer auf eine andere Baureihe oder gar einen anderen Hersteller übertragen.

Zudem sichern die Hersteller ihre Bordnetze zunehmend besser ab, sagt Wolf. In die Autoelektronik integrierte Hardware-Firewalls sollen bei den neuesten Modellen dafür sorgen, dass Angreifer nicht allzu weit

WLAN-HOTSPOTS BIETEN EINE ANGRIFFSFLÄCHE.

vordringen können. Und in manchen Bord-Netzwerken werden Datenpakete bereits verschlüsselt. Doch Wolf warnt auch vor zu viel Vertrauen in die Technikhürden. „Hundertprozentigen Schutz gibt es nicht. Mit genügend Aufwand lässt sich jedes System umgehen“, meint er.

Auch steigt die Zahl der möglichen Angriffsflächen. Denn die vernetzten Autos, die gute Geschäfte versprechen, haben auch ihre Schattenseiten. So lassen sich einige Neuwagen gegen Aufpreis mit WLAN-Hotspots hochrüsten. Auf langen Autofahrten ist das speziell für die Mitfahrer auf der Rückbank angenehm – sie können nach Eingabe eines Passworts problemlos via Handy oder Tablet im Internet surfen. Unter Sicherheitsfachleuten gilt die WLAN-Technik allerdings nicht als besonders einbruchssicher. Über solche standardisierten Schnittstellen können Hacker in ein Umfeld eindringen, das Daten mit den internen Netzwerken im Auto austausche, warnen Experten.

Zwar ist die Reichweite der WLANs im Auto eher gering. Angreifer müssten schon über längere Strecken sehr nahe an ein Auto heranfahren, um die drahtlose Kommunikation abzufangen und weiter eindringen zu können. Doch die WLAN-Hotspots im Auto bieten eben grundsätzlich eine weitere mögliche Angriffsfläche.

Für bedenklich halten Fachleute auch die Verschmelzung von Smartphone und Bordelektronik. Google und Apple möchten ihre Mobil-Betriebssysteme fest in Autos verankern. Denn so können sie Apps optimal für die Darstellung in den Auto-Displays anpassen, ihre Smartphones lassen sich dann viel komfortabler steuern. Schon nächstes Jahr wollen Audi, BMW und Mercedes Fahrzeuge ausliefern, die Apples iOS oder Googles Android an Bord haben. „Vom Komfortaspekt her ist das toll, unter Sicherheitsaspekten jedoch alles andere als sinnvoll“, sagt Marco Lux, Geschäftsführer des IT-Sicherheitsunternehmens Curesec.

Für die Fahrer böte das autointerne Betriebssystem Vorteile, weil sie so via Smartphone leichter auf einige interne Funktionen zugreifen könnten. Bereits heute lässt sich bei manchen Herstellern über das Smartphone etwa die Standheizung ein- und ausschalten oder die Tankanzeige ablesen. Künftig könnte ein Fahrer auch vor einem Parkplatz aussteigen und sein Auto per Smartphone-App in die Lücke dirigieren.

„Wenn das Telefon direkt mit Steuerungssystemen verbunden ist, wird es spannend“, sagt Lux. Noch ist es nicht so weit – und es bleibt fraglich, wie weit Hacker nach einem gelungenen Einbruch tatsächlich zu den kritischen Systemen vordringen können, die etwa die Lenkkraftverstärkung oder das Bremsverhalten regeln. Denn Autobauer schotten ihre bordinternen Unterhaltungssysteme vom Rest der Bordelektronik nicht nur mit Firewalls, sondern auch mit anderen speziellen Softwaremaßnahmen ab.

Allerdings gibt es dabei große Unterschiede zwischen den Herstellern, wie eine Untersuchung der US-Sicherheitsexperten Charlie Miller und Chris Valasek zeigt. Sie haben knapp zwei Dutzend Automodelle auf mögliche Schwachstellen in ihrer Sicherheitsarchitektur untersucht. Der 3er-Serie von BMW, dem Hybridauto i8 und dem Audi A8 bescheinigte die Studie eine nur schwer manipulierbare Netzwerkarchitektur. Der Jeep Cherokee, Cadillacs Riesen-SUV Escalade und Infinitis Nobellimousine Q50 bieten dagegen ziemlich viel Angriffsfläche, erklärten die Studienautoren.

DIE ERGEBNISSE sorgten für Aufsehen, weil Miller und Valasek bereits im Jahr 2013 der Autobranche einen Spiegel vorhielten. Per angeschlossenem Kabel drangen die beiden in das Bordnetz ihres Toyota Prius ein und manipulierten die Bordelektronik so weit, dass sie Lenkung und Bremsen bei voller Fahrt vom Laptop aus steuern konnten. Die Idee findet offenbar Nachahmer. Auf der Plattform Kickstarter suchte der Amerikaner Derek Kuschel Sponsoren für ein Gerät namens CANBus Triple. Es soll die Steuersignale elektronischer Geräte von Autos lesen und verändern können – per Verkabelung mit der sogenannten Diagnosebuchse, in die in der Regel Werkstätten ihre Computer zur Fehleranalyse einstöpseln.

Ob sich damit auch etwa Bremsen oder die Motorsteuerung beeinflussen lassen, verrät Kuschel nicht. Doch möglich ist das, meint ein deutscher Experte, der im Auftrag von Herstellern bereits meh-

rere Modelle gehackt hat. „Normalerweise dürfen sie diese Diagnoseschnittstellen nicht während der Fahrt verwenden – dennoch ist das mit ein paar Tricks bei vielen Autos möglich." Letztlich kann man damit auch in die Steuerung eingreifen, sagt er. „Ich kann damit eine Bremsaktion auslösen oder die Parameter für den Lenkkraftverstärker verändern."

Dennoch hält auch er solche Angriffe für wenig wahrscheinlich. Um wirklich volle Kontrolle über ein einziges Fahrzeug zu erlangen, sei wochenlange Arbeit notwendig – und der finanzielle Aufwand dafür sei hoch. „Diese Angriffe sind teurer als alle anderen Möglichkeiten. Wenn jemand gegen den Baum fahren soll, ist es einfacher, die Bremsschläuche durchzuschneiden", meint er.

Es ist die Beweglichkeit der Autos, die sie nach Meinung von Experten bislang noch schwerer angreifbar macht als PCs und Tablets. Diese laufen oft stundenlang, bevor sie ausgeschaltet werden, meist mit einer ständigen Internetverbindung. Auf ihnen lassen sich vergleichsweise einfach Schadsoftware in Form von Apps installieren. Der Nutzer muss nur in einem unbedachten Moment zustimmen.

Autos werden dagegen viel öfter an- und abgeschaltet – und noch sind erst wenige Neuwagen internetfähig. Ist die Zündung erst mal aus, wird meist auch die Netzverbindung getrennt. Zudem ist die Installation von Apps an Bord bisher nur sehr eingeschränkt und in geringem Umfang möglich. Doch das dürfte sich in den nächsten Jahren ändern.

Denn alle großen Hersteller arbeiten mit Hochdruck daran, speziell auf Autos zugeschnittene Apps zu entwickeln und an Bord nutzbar zu machen. Und die Zahl der mit dem Internet verbundenen Fahrzeuge wird rasant ansteigen. In drei Jahren werden bereits 60 Prozent aller Neuwagen weltweit mit Internetzugang ausgeliefert, schätzt die Unternehmensberatung ABIresearch. In Europa dürften es wohl noch deutlich mehr werden. Denn bereits ab Oktober 2015 soll jeder europäische Neuwagen ein automatisches Notrufsystem namens eCall an Bord haben. Das System setzt bei einem Verkehrsunfall einen Notruf ab, wenn der Airbag ausgelöst wurde oder der Fahrer die Notruftaste drückt. Dabei wird auch eine Sprachverbindung in das Auto aufgebaut. Zugleich werden die genauen Koordinaten des Unfallorts, die Fahrtrichtung und die Fahrzeug-ID übermittelt. Zusätzlich ist auch die Übertragung von Daten aus dem Bord-Sicherheitssystem möglich.

Zwar baut eCall erst bei einem Unfall eine Verbindung auf, es sendet also nicht permanent Daten nach draußen. Doch das System verfügt nicht nur über GPS- und Mobilfunkmodule, es hat auch Zugriff auf einige Daten aus dem internen Fahrzeugnetzwerk. Die EU-Vorgaben sehen zudem vor, dass Hersteller parallel zum eCall-System eigene Zusatzdienste anbieten können.

DAS ECALL-SYSTEM hat einen hohen Sicherheitsstandard, meinen Experten. Doch die Zusatzdienste öffnen ein weiteres Einfallstor. Deutschlands Autohersteller äußern sich nur zurückhaltend zum Thema IT-Sicherheit im Auto – denn sie fürchten dabei um ihren guten Ruf. Die Branche ist sensibilisiert. „Wenn es um das Thema Internet geht, ist bei allen Herstellern der Schutz vor Manipulation mittlerweile ein zentrales Thema", meint Escrypt-Mann Wolf, auch wenn diese über konkrete Sicherheitsmaßnahmen aus Wettbewerbsgründen ungern reden. Dabei setzen die Autohersteller durchaus auch auf Hilfe von außen. Mercedes etwa hat Sicherheitsexperten mit dem Hacken der S-Klasse beauftragt. Der Luxuskreuzer erwies sich laut Daimler-Angaben als harte Nuss. Drei Monate lang versuchten die Hacker, die Bordelektronik zu knacken – und scheiterten.

Der US-Autohersteller Tesla geht einen anderen Weg: Auf der Hackerkonferenz Def Con lud Tesla-Chef Elon Musk dazu ein, elektronisch in sein Modell S einzubrechen. Den 20 bis 30 besten Hackern versprach er einen Job im Unternehmen. Und die Hackerszene geht ihrerseits auf die Hersteller zu. Mitte August hat eine Gruppe Spezialisten die Autobauer zur Zusammenarbeit ermuntert. Die Gruppe „I Am The Cavalry" fordert von den Herstellern, die IT-Sicherheit von Anfang an in die Entwicklung neuer Technologien einzubeziehen – und zwar so, dass es Außenstehende auch nachvollziehen können.

Fehler sollen systematisch aufgezeichnet werden, meint die Gruppe. Sicherheits-Updates einfach und schnell möglich sein. Zudem verlangen die Hacker, dass Netzwerkarchitekturen im Auto so getrennt sein müssen, dass etwa ein Angriff auf das Infotainmentsystem nicht auf kritische Systeme wie Bremsen durchschlagen kann. Eine offizielle Stellungnahme eines Autoherstellers zu den Hackerforderungen liegt bislang aber noch nicht vor. ■