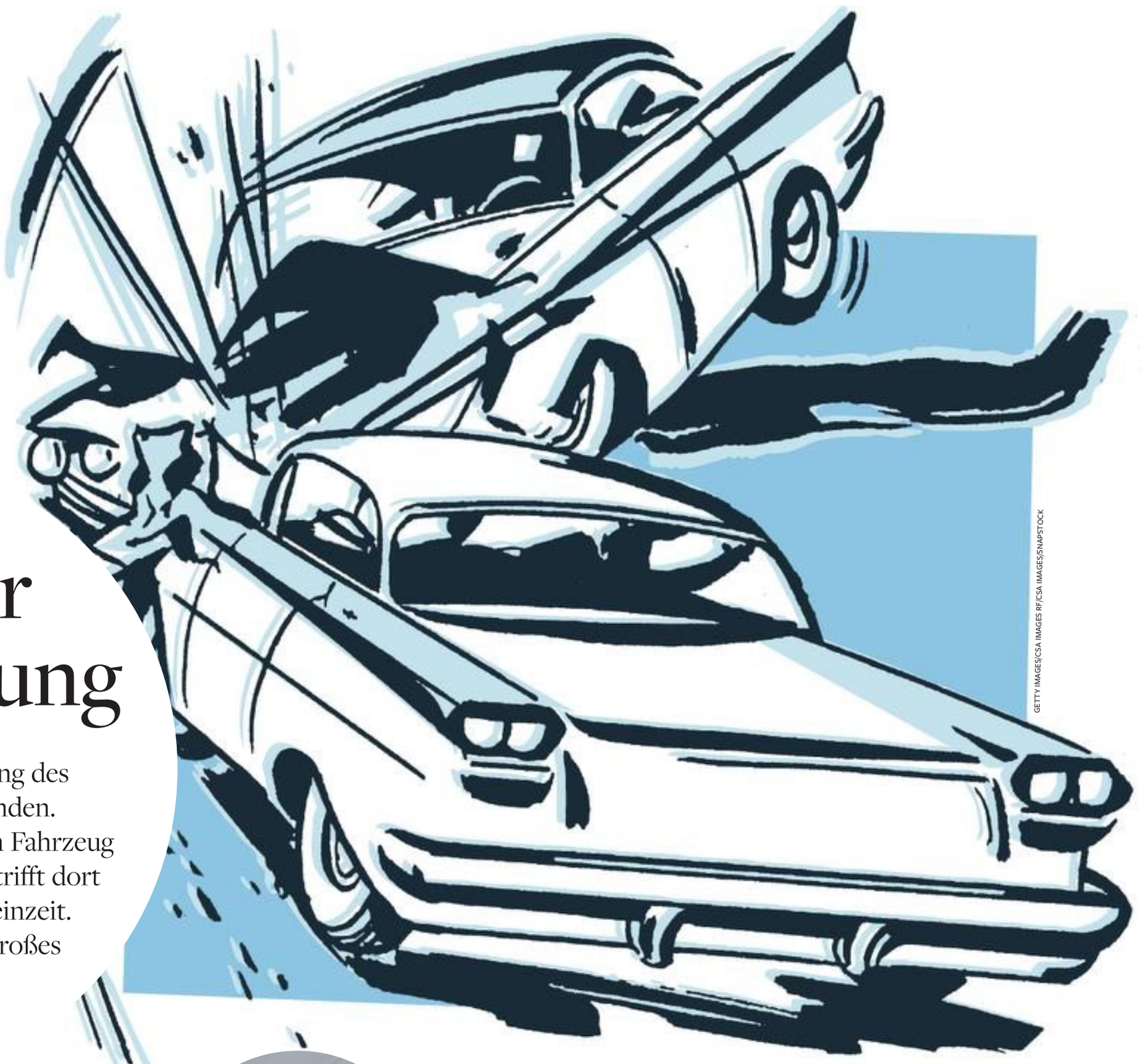
Superrechner „Mistral“
Frischer Wind aus Hamburg für die globale Klimaforschung **Seite 2**

DIE WELT

Smart Homes
Die Technik existiert, doch nicht alle Elemente werden nachgefragt **Seite 4**

DIENSTAG, 17. NOVEMBER 2015

SONDERAUSGABE VERNETZTE WELTEN



GETTY IMAGES/CSA IMAGES RF/CSA IMAGES/SNAPSTOCK

Crash per Fernsteuerung

Das Auto wird oft als Erweiterung des eigenen Wohnzimmers empfunden. Doch wer sein Smartphone mit dem Fahrzeug verbindet, sollte wissen: Hightech trifft dort auf Technik aus der digitalen Steinzeit. Und diese bietet ein scheunengroßes Einfallstor für Hacker

BJÖRN ENGEL

Ich ist ein Anderer, heißt es bei Arthur Rimbaud. Der französische Dichter des 19. Jahrhunderts war dabei alles andere als ein Autoknacker. Und doch hat Rimbaud mit dieser Zeile vorweggenommen, womit heute angesichts der digitalen Vernetzung die Hersteller zu kämpfen haben: Mit Profilen, die ausgeben, jemand zu sein, der sie nicht sind.

„Die Fahrzeughersteller kämpfen damit, dass viele ihre privaten Kommunikationsgeräte wie zum Beispiel Smartphones mit dem eigenen Auto vernetzen wollen“, sagt Professor Eric Hilgendorf, der an der Uni Würzburg Robotrecht lehrt und die Bundesregierung berät. Laut einer Umfrage der Management- und Technologieberatung BearingPoint wünschen sich 47 Prozent der potenziellen Autokäufer mobile Online-Dienste wie Verkehrsinformationen in Echtzeit oder digitale Entertainment-Angebote für ihr neues Fahrzeug. „Wir erwarten, dass ein Autokauf in Zukunft noch stärker von der Verfügbarkeit mobiler Dienste beeinflusst wird“, sagt Matthias Loebich, der den Bereich Automotive leitet.

Das klingt erst einmal nur nach einem Verkaufsargument und weniger nach einer Bedrohung. Leider ist das Gegenteil der Fall. Grund dafür ist die zum Teil veraltete Technik, die noch heute in Neufahrzeugen verbaut wird. Größtes Scheunentor ist der CAN-Bus, das „Controller-Area-Network“-Bussystem, das 1983 von Bosch entwickelt wurde, um Steuergeräte in Autos zu vernetzen und gleichzeitig dadurch auf mehrere Kilometer Kabel verzichten zu können.

Dieser CAN-Bus war so erfolgreich, dass er fortan in quasi jedes Fahrzeug eingebaut wurde. Seine Bedeutung ist auch heute noch für jeden sofort sichtbar, der sein Auto in die Werkstatt bringt: Dort sieht man in der Regel den Meister und seine Gehilfen im Blaumann vor Monitoren stehen, auf denen sie zum Beispiel die Fehlerspeicher des Fahrzeugs auslesen. Dazu haben sie sich vorab per Kabel und Stecker mit dem Diagnose-Port des CAN-Busses verbunden.

Der CAN-Bus ist also ein Meilenstein des Automobilbaus. Nur ist das System ein Meilenstein aus den Anfängen der Digitalisierung und heute gegen Angriffe von Außen schlicht überfordert. Andreas Mai, zuständig bei Cisco Systems für den Bereich „Connected Cars“ erläutert: „Der CAN-Bus ist einer der großen Schwachpunkte in Fahrzeugen, denn das CAN-Protokoll hat nur acht Bit, die minimale Verschlüsselungs-Technologie erfordert aber 128 Bit.“

Ein Code aus acht Bit ist ein Befehl aus einer achtstelligen Zahlenfolge von 0 und 1, etwa 10101010. Mehr Kapazität hat der CAN-Bus nicht. Um wirkungsvoll zu verschlüsseln, müsste er aber Zahlenfolgen verarbeiten, die 16 Mal so lang sind. Das lässt nun die Datenrate des CAN-Busses nicht zu, weshalb das Bussystem für blinde Passagiere weitgehend offen ist.

Doch wie kommen diese an Bord? Wie ist es möglich, die Motorsteuerung anzugreifen und Autos nach der eigenen Pfeife tanzen zu lassen? Derzeit gibt es speziell zwei prominente Möglichkeiten, Gewalt über ein Fahrzeug per digitalem Zugriff zu erlangen. Einmal über einen „Dongle“, einen speziellen Stecker, der auf den Diagnose-Port kommt und per Bluetooth funken kann. Ein anderes Einfallstor ist das Smartphone, das entweder über Funk oder per USB-Schnittstelle mit der Entertainment-Einheit des Fahrzeugs verbunden wird.

Auch wenn solche Dongles nicht jedermann gleichermaßen bekannt sind wie etwa Smartphones, erfreuen sie sich zunehmender Beliebtheit. „Es gibt schon eine ganze Reihe von Start-ups wie Zubie, Automatic oder Vinli, die einen kleinen Dongle entwickelt haben, der die Abfrage von Diagnosedaten ermöglicht. Diese werden dann aufs Smartphone übertragen, um zum Beispiel zu sehen, ob irgendwelche Probleme mit dem Fahrzeug bestehen oder um die Performance ablesen zu können“, sagt Mai.

Selbst ein Discounter wie Lidl bietet in Deutschland so ein Gerät für keine 50 Euro auf seiner Internetseite an. Ein solcher Stecker kann, einmal mit dem CAN-Bus verbunden, den Fehlerspeicher auslesen, die Bordspannung live ebenso angeben wie die tatsächliche Geschwindigkeit, Öltemperatur oder den Öldruck. Die Daten werden in Echtzeit für Smartphone- oder Tablet-Apps aus den App-Stores von Apple oder Google grafisch aufbereitet und per Bluetooth auf die entsprechenden Geräte übertragen. Ebenfalls eine Funkverbindung zur Umgebung bauen Smartphones auf, die einfach zum Beispiel an die Audioanlage im Fahrzeug angeschlossen werden.

Potenzielle Hacker fangen nun diese Funksignale auf, wobei spezielle Software ihnen hilft, die Kommunikation zwischen einem Smartphone oder Dongle und einem Fahrzeug zu identifizieren. Gefährlich wird es besonders dann, wenn das Smartphone die unverschlüsselte Anfrage an den Access Point, in diesem Fall also die Schnittstelle vom CAN-Bus, stellt. Dabei senden Dongle oder Smartphone ihre MAC-Adresse. Diese hat nichts mit den gleichnamigen Apple-Produkten zu tun, sondern ist eine einmalige „Media-Access-Control“-Adresse, die jeder einzelnen Hardware zugeordnet ist und mit der diese identifiziert werden kann.

Wurde die MAC-Adresse abgefangen, kann sie leicht kopiert werden: Ich ist nun ein anderer. Und da das Original und der Access Point aufgrund der Konstruktionsweise des CAN-Bus keine Verschlüsselung miteinander vereinbaren konnten, hat der Hacker nun Zugriff auf die Motorsteuerung. Stets vorausgesetzt, dass diese nicht physisch vom Entertainment abgeschottet wurde – ein teurer Aufwand, der bislang eigentlich nur in der Luxusklasse betrieben wird.

„Die zentrale Frage des Datenschutzes lautet: Sind die Autohersteller in der Lage, dem Kunden eine mit dem Smartphone vergleichbare Funktionalität im Auto zu bieten und gleichzeitig die optimale Sicherheit zu gewährleisten?“, fragt sich Loebich. Das sei so lange mit überschaubarem Aufwand möglich, solange es sich um ein proprietäres, also ein abgeschottetes System handele. „Wenn es aber um standardisierte Dienste geht, müssen sich die Hersteller öffnen.“

Doch eine weitere Öffnung bedeutet, dass die Motorsteuerung noch besser geschützt werden muss, was nur Ethernet vermag. Ethernet, das heute noch deutlich teurer als die CAN-Bus-Technik ist, stellt die Bandbreite zur Verfügung, mit der Verschlüsselungen umsetzbar sind. Weil die Zahl der Fahrassistenzsysteme stetig steigt, die bei Autos wie dem BMW 7er oder der Mercedes S-Klasse autonomes Fahren im Ansatz schon ermöglichen, ist es nur eine Frage der Zeit, bis Ethernet überall Einzug hält. „Das Ethernet bietet die Bandbreite, die Videoübertragungen an Bord erst ermöglicht“, sagt Mai. Diese Übertragungen sind bereits heute bei Fahrzeugen nötig, die etwa die Straße im Kameraauge behalten, um ein mögliches Abweichen aus der Spur zu korrigieren. Dazu muss so ein System wenigstens mit der Bremsanlage und der Lenkung kommunizieren. Das verlangt deutlich mehr Datengeschwindigkeit als die, die ein CAN-Bus verarbeiten kann.

> „Der CAN-Bus ist einer der großen Schwachpunkte in Fahrzeugen“
>
> **Andreas Mai,** Experte für „Connected Cars“ bei Cisco Systems

Er ist eine Schwachstelle – und nur einer von vielen Angriffspunkten. Derzeit versucht die Autoindustrie mit „White Lists“, die die Kommunikation nur für bestimmte „Messages“ und zwischen bestimmten elektronischen Kontrollsystemen zulässt, mögliche Lücken zu schließen. Bis das vollständig gelingt, können Hacker sich Zugang verschaffen, die CAN-Bus-Protokolle lesen, Befehle senden und so auch während der Fahrt Kontrolle über ein Fahrzeug erlangen. Hacks sind bislang nur vereinzelt und Spezialisten mit hohem Zeitaufwand gelungen. „Aber unter Experten ist es unstrittig, dass die Gefahr groß ist und weiter zunehmen wird“, sagt Hilgendorf. Ich ist dann nicht nur ein Anderer, es ist dann auch ein anderes Ich, das mein Auto steuert.

Die Inhalte dieser Beilage unter: www.welt.de/vernetzte-welten

Autos und Smartphones sind eine beeindruckende Verbindung. Schon heute gibt es Fahrzeuge wie von Audi (Foto Mitte), denen per Smartphone der Befehl zum Einparken gegeben werden kann. Umgekehrt können Funkverbindungen leicht abgefangen werden

GETTY IMAGES (4)

> „Ein Autokauf wird in Zukunft noch stärker von der Verfügbarkeit mobiler Dienste beeinflusst“
>
> **Matthias Loebich,** Leiter Automotive bei BearingPoint