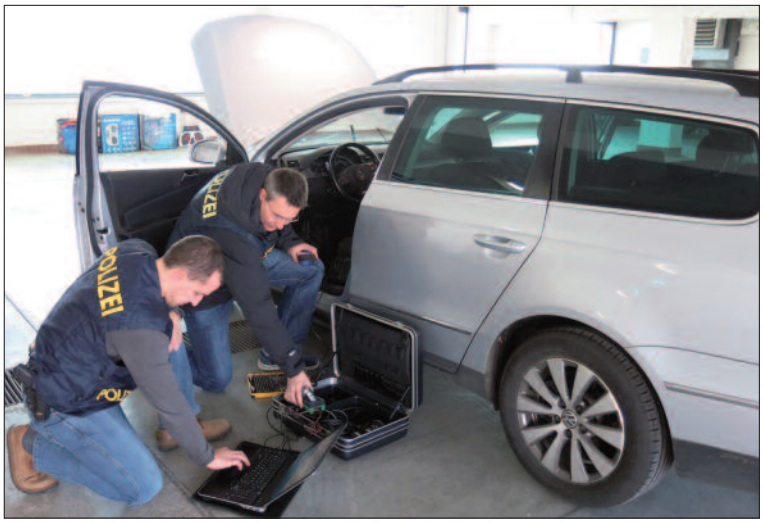
Beweismittel Auto

Kraftfahrzeuge speichern beim Betrieb Daten und senden sie oft an den Hersteller. Diese Daten ermöglichen es der Polizei, eine Straftat oder den Hergang eines Unfalls aufzuklären.

Ein Autobesitzer erstattete am Morgen des 16. Juni 2015 in Linz bei der Polizei eine Anzeige, weil sein Fahrzeug nicht mehr war, wo er es am Tag zuvor abgestellt hatte. Die Polizei schrieb das Fahrzeug zur Fahndung aus. Noch am selben Tag wurde das Auto in Prag von der Polizei sichergestellt und der Fahrzeugdieb wurde festgenommen. „Wir haben das Auto untersucht und festgestellt, dass der Dieb ohne Gewaltanwendung in das Fahrzeug gelangt war und es mit einem selbst programmierten Nachschlüssel in Betrieb genommen hat“, berichtet Kontrollinspektor Horst Reisner, MSc, vom *Cybercrime-Competence-Center (C4)* des Bundeskriminalamts.

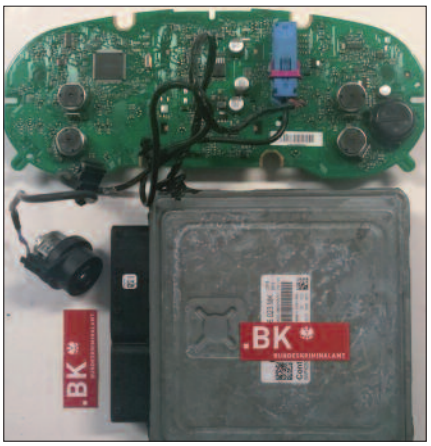


„Cybercops“ Armin Rauchbüchl und Horst Reisner bei der forensischen Untersuchung eines sichergestellten Autos.

Überwindbare Elektronik. Wer glaubt, ein Auto, das mit vielen elektronischen Komponenten ausgestattet ist, sei sicherer vor Diebstahl, der irrt. Längst ist es Kriminellen möglich, das Signal eines Transponderschlüssels abzufangen oder zu blockieren, die elektronische Wegfahrsperre zu deaktivieren oder einen Fahrzeugschlüssel-Rohling zu programmieren. Innerhalb weniger Minuten gelingt es Dieben, ein Fahrzeug ohne Beschädigung zu öffnen und zu stehlen.

Die Manipulationen am Fahrzeug und an Steuergeräten werden oft von der Bordelektronik aufgezeichnet. Das kann der Polizei bei der Ermittlung der Täter oder bei der Rekonstruktion von Unfällen hilfreich sein. Die elektronischen Komponenten eines Fahrzeugs sind vom Hersteller meistens nicht ausreichend vor missbräuchliche Verwendung geschützt. Jeder kann zum Beispiel ein Diagnosegerät kaufen, mit dem man bestimmte Informationen eines Fahrzeugs auslesen kann, die im Fehlerspeicher gesichert sind. Werkzeuge zur Manipulation von Steuerungsgeräten oder Schlüsselkopiergeräte kann man über das Internet kaufen. „Wir haben gemeinsam mit der Soko Kfz sichergestellte Autos untersucht, die aus verschiedenen, vermutlich gestohlenen Teilen zusammengebaut worden sind“, berichtet Reisner. Durch Auslesen der Steuerungsgeräte stellten die Ermittler fest, dass die verschiedenen Fahrzeugteile an die Bordelektronik bzw. an das Fahrzeugsystem „angelernt“ worden waren. Man kann außer einem Schlüsselrohling auch weitere Fahrzeugbestandteile „anlernen“, wie Airbags, Navis, Getriebe und Klimaanlagen.

EU-Projekt. Horst Reisner und seine Kollegen Armin Rauchbüchl und Robert Lang vom *C4* arbeiten seit September 2014 im von der EU finanzierten Projekt „Fahrzeugforensik – Forensische Untersuchung von IT-Systemen und Datenspeicher in Kraftfahrzeugen zur Klärung von Straftaten“. Die Idee, sich näher mit der Auswertung von Fahrzeuginformationen zu beschäftigen, kam den IT-Forensikern und Cybercrime-Ermittlern bei der täglichen Arbeit. „Wir haben bei der forensischen Untersuchung von Autos festgestellt, dass man aus den Steuerungselementen mehr Informationen herauslesen kann, als es mit einem herkömmlichen Fahrzeug-Diagnosegerät möglich ist“, betont Reisner. Sensoren, elektronische Bauteile und Bus-Systeme in Fahrzeugen können durch Analyse und Auswertung wichtige Informationen über den Betriebszustand des Fahrzeugs und damit einen elektronischen Sachbeweis für Gerichtsverfahren liefern.

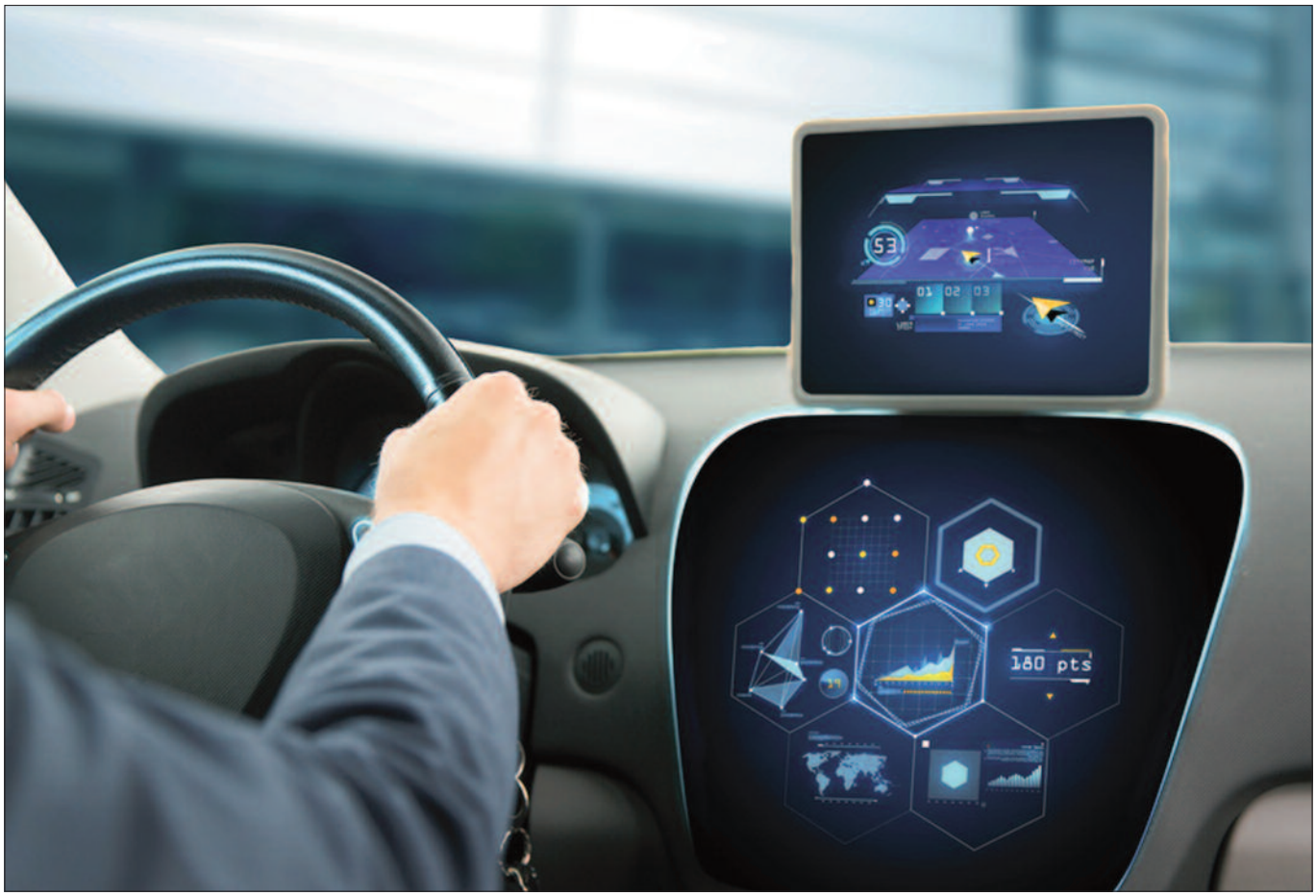


Steuerungsgerät: Speicherung von Informationen über Fahrzeug und Betrieb.

Ein Daten-Bus ist ein System zur Datenübertragung zwischen mehreren Teilnehmern über einen gemeinsamen Übertragungsweg. Datenbusse, auch *Controlled Area Network (CAN)* genannt, verbinden bis zu 100 verschiedene Steuermechanismen miteinander. Ein Teil dieser Daten wird im Fehlerspeicher des Autos abgelegt und liefert bei einer Fahrzeugpanne Informationen über Defekte. Darüber hinaus zeichnen Sensoren das individuelle Fahrverhalten, Betriebszustände, Fehlerquellen und Bedienungsschritte des Fahrers während des Fahrens auf.

Autoschlüssel eines bestimmten Herstellers speichern Informationen wie die Fahrzeugidentifikationsnummer (VIN), den Kilometerstand, den Tankinhalt, die Innen- und Außentemperatur, die Transponder-ID und mehr. Diese Informationen können für kriminalpolizeiliche Ermittlungen von Bedeutung sein. Ziel des Projekts ist die Errichtung einer zentralen Servicestelle zur kriminalpolizeilichen Beweismittelsicherung von Kfz-Daten („Fahrzeugforensik“) im BMI.

FOTOS: BUNDESKRIMINALAMT/THOMAS RATHPOLLER



Vernetzte Autos: Das Speichern und Senden von Informationen an den Fahrzeughersteller erfolgt in einem rechtlichen Graufeld.

Manipulationen. Mit einer Auslese- und Diagnosesoftware ist es möglich, Informationen über den Betrieb des Fahrzeuges und über verbaute Bestandteile zu erlangen. Dazu zählen unter anderem das Auslesen von GPS-Koordinaten, das Erkennen einer Manipulation des Kilometerstands, die Feststellung, ob die Leistung eines Fahrzeugs verändert worden ist („Chiptuning"), ob es Manipulationen an der Bordelektronik gegeben hat, ob Fahrzeugteile von anderen (gestohlenen) Fahrzeugen eingebaut, nachträglich ein Fahrzeugschlüssel angelernt oder die elektronische Wegfahrsperre deaktiviert worden ist. Die IT-Komponenten in einem Fahrzeug haben keine Firewall, sie sind nicht gesichert. Hacker können beispielsweise in elektronische Systeme eines Fahrzeugs eindringen und die Steuerung des Fahrzeugs übernehmen und die Bremsen blockieren.

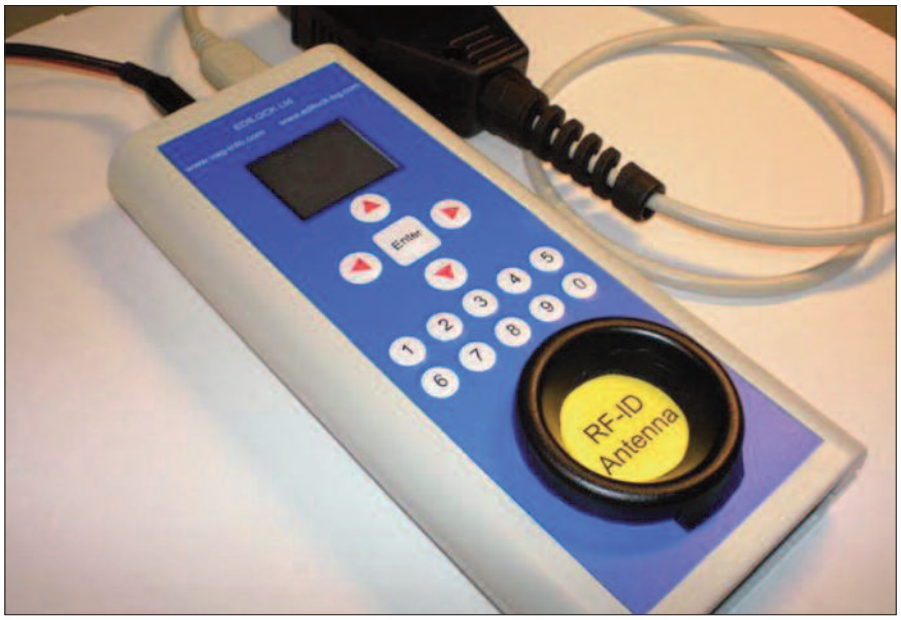
Zeit-Weg-Diagramme. Aus Navigationsgeräten und Smartphones lassen sich beweiskräftige Informationen auswerten. Waren aber die Mobilgeräte während der Tatbegehung ausgeschaltet, kann man möglicherweise immer noch erkennen, dass der Tatort davor unter Verwendung des Navis ausgekundschaftet worden ist. „In diesem Fall kann möglicherweise über die Auswertung von Fahrzeugdaten ein Bezug zum Tatort und der Straftat hergestellt werden", erläutert Horst Reisner.

Unfallrekonstruktion. Ein weiteres Einsatzgebiet der Kfz-Forensik ist die Rekonstruktion der Geschehnisse vor, während und nach einem Unfall. Speziell bei Unfällen mit Todesfolge können wichtige Informationen zur Klärung des Unfallhergangs ausgelesen werden. Häufig behaupten Zeugen, dass der Lenker zum Unfallzeitpunkt ohne Freisprecheinrichtung telefoniert habe. In diesem Fall können die Rufdaten vom Mobilfunkbetreiber den Nachweis erbringen, ob ein Gespräch mit dem Mobilgerät zum Unfallzeitpunkt getätigt worden war. Sie lassen aber keinen Rückschluss zu, auf die Benutzung einer Freisprecheinrichtung oder die Ablenkung des Lenkers durch Bedienung des Entertainment-Systems. Das kann durch Auswertung der Fahrzeugdaten geprüft werden. Elektronisch verstellbare Vordersitze speichern nicht nur die Sitzposition des Fahrers und Beifahrers, sondern auch deren Gewicht. „Wenn jemand behauptet, er habe das Fahrzeug zum Unfallzeitpunkt nicht gelenkt, kann man das aufgrund der gespeicherten Gewichtsdaten überprüfen", sagt Armin Rauchbüchl.

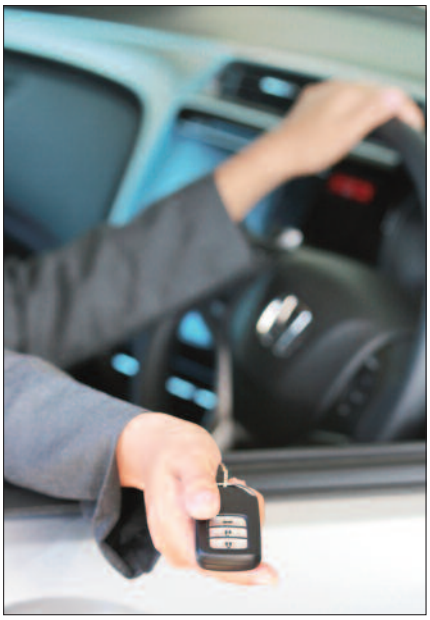
Vernetzte Autos. Fahrzeuge können mit anderen Fahrzeugen kommunizieren. Mobile Geräte wie Smartphones oder Tablets werden immer öfter mit dem Auto vernetzt. Es gibt eine Reihe nützlicher Assistenzsysteme in neuen Fahrzeugen wie Gefahrenwarnung, Spurhaltesysteme, Kreuzungsassistent und automatischer Notruf bei einem Unfall.

Die Steuerungsgeräte im Fahrzeug kommunizieren nicht nur untereinander, sie sind auch mit dem Hersteller und mit dem Internet verbunden. Viele dieser Daten sind personenbezogen und lassen zum Beispiel Rückschlüsse auf das Fahrverhalten und Aufenthaltsorte zu. Die Zunahme von IT-Komponenten in einem Fahrzeug birgt auch Gefahren in Bezug auf Datenschutz und Datensicherheit sowie auf IT-Sicherheit. „In der Anfangszeit der WLAN-Geräte hat

FOTO: FOTOLIA/SYDA PRODUCTIONS



Fahrzeugschlüssel-Kopiergerät: Werkzeuge zur Manipulation von Kraftfahrzeugen werden über das Internet angeboten.



Auch Autoschlüssel speichern Informationen über das Fahrzeug.

sich fast niemand um Sicherheit gekümmert", sagt IT-Forensiker Horst Reisner. „Erst mit der Zeit hat man darauf geachtet, WLAN-Systeme zu verschlüsseln." Reisner sieht dieses Manko auch mit der IT- und Internet-Verbundenheit von Fahrzeugen. Es gibt nahezu keine IT-Sicherheit in Fahrzeugen. Steuergeräte und Multimedia-Komponenten sind wenig gesichert vor Angriffen von außen.

Umfrage. Der Automobilweltverband *FIA (www.fia.com)* hat die Kampagne *„My Car My Data" (www.mycarmydata.eu)* gestartet. Damit soll das Bewusstsein für den Schutz sensibler Daten bei vernetzten Autos geweckt werden. Dafür ließ der Verband im August 2015 in Europa untersuchen, welche Daten zwei Neufahrzeuge – ein Diesel- und ein Elektrofahrzeug – erfassen und an Werkstätten, Pannenhelfer und Hersteller übermitteln. Der Datentransfer erfolgte über eine eingebaute SIM-Karte oder über die App des Autoherstellers am Smartphone. Neben Fahrerprofil, Fahrzeugortung und Fahrzeit wurden die vom Mobiltelefon synchronisierten Daten im Speicher abgelegt. Parallel zum Fahrzeugtest führte *FIA* im Oktober 2015 eine Online-Befragung von 12.000 Teilnehmern in zwölf europäischen Ländern durch, darunter Österreich. 95 Prozent der Befragten forderten gesetzliche Regelungen für den Datentransfer von und zu einem Pkw; 91 Prozent wünschten sich die Möglichkeit, die Kommunikation abzuschalten; 92 Prozent möchten damit verbundene Angebote für Pkw-Dienstleistungen herstellerunabhängig wählen können. 86 Prozent der 1.000 befragten Österreicher sind bereit, Daten zur Pannenbehebung weiterzugeben; 91 Prozent wollen den Pannendienst selbst wählen; 97 Prozent wollen die Kommunikation aus dem Auto abschalten können.

In Österreich besitzen nur fünf Prozent ein „connected Car", ein vernetztes Auto. Die Quote steigt, weil die Hersteller diese Elektronik auch in Mittel- und Kleinwagen einbauen. Im Vergleich mit den anderen EU-Bürgern sind die Österreicher laut der Online-Umfrage nicht nur gut informiert, sie sind auch besorgter, was die kommerzielle Nutzung ihrer Daten sowie mögliche Hackerangriffe betrifft. 92 Prozent der Österreicher sehen laut der *FIA*-Umfrage Bedarf für gesetzliche Regelungen. *Siegbert Lattacher*

PRÄVENTION

Elektronische Sicherung

OBD-Saver. Über das On-Board-Diagnose-System (OBD) könnte ein Dieb die elektronische Wegfahrsperre deaktivieren. Ein OBD-Saver schützt den Stecker und kann einen unbefugten Zugriff auf die Elektronik und Steuergeräte des Kraftfahrzeugs verhindern.

Unterbrecher. Individuelle Stromunterbrechungen werden versteckt im Fahrgastraum eingebaut. Der Lenker kann die Elektrik (Zündspule, Anlasser, Benzinpumpe) auf Knopfdruck unterbrechen, bevor er aussteigt. Der Motor lässt sich nicht starten. Autodieben fehlt meist die Zeit, die Stromtaste zu suchen.

Alarmanlagen sollten nach dem Verlassen des Fahrzeuges immer eingeschaltet werden und einfach zu bedienen sein. Die Anlage sollte nur von Fachwerkstätten eingebaut werden, weil der Einbau kompliziert ist und die Alarmanlage genau eingestellt werden muss.

Ortung. Mit einem Ortungssystem kann der momentane Standort eines gestohlenen Kraftfahrzeugs abgerufen werden, wodurch die Chance auf die Auffindung steigt. Mittlerweile gibt es verschiedene Anbieter, die nach einem Diebstahl in der Regel länderübergreifend mit Polizeibehörden zusammenarbeiten.

Zentralverriegelung. Beim Abstellen des Fahrzeugs sollte man sich immer vergewissern, dass es auch tatsächlich versperrt ist. Diebe können mit Störsendern das automatische Schließsignal des Funkschlüssels unterbinden, sodass der Wagen geöffnet bleibt.

Fotos: Bundeskriminalamt, Fotolia/Kokotewan