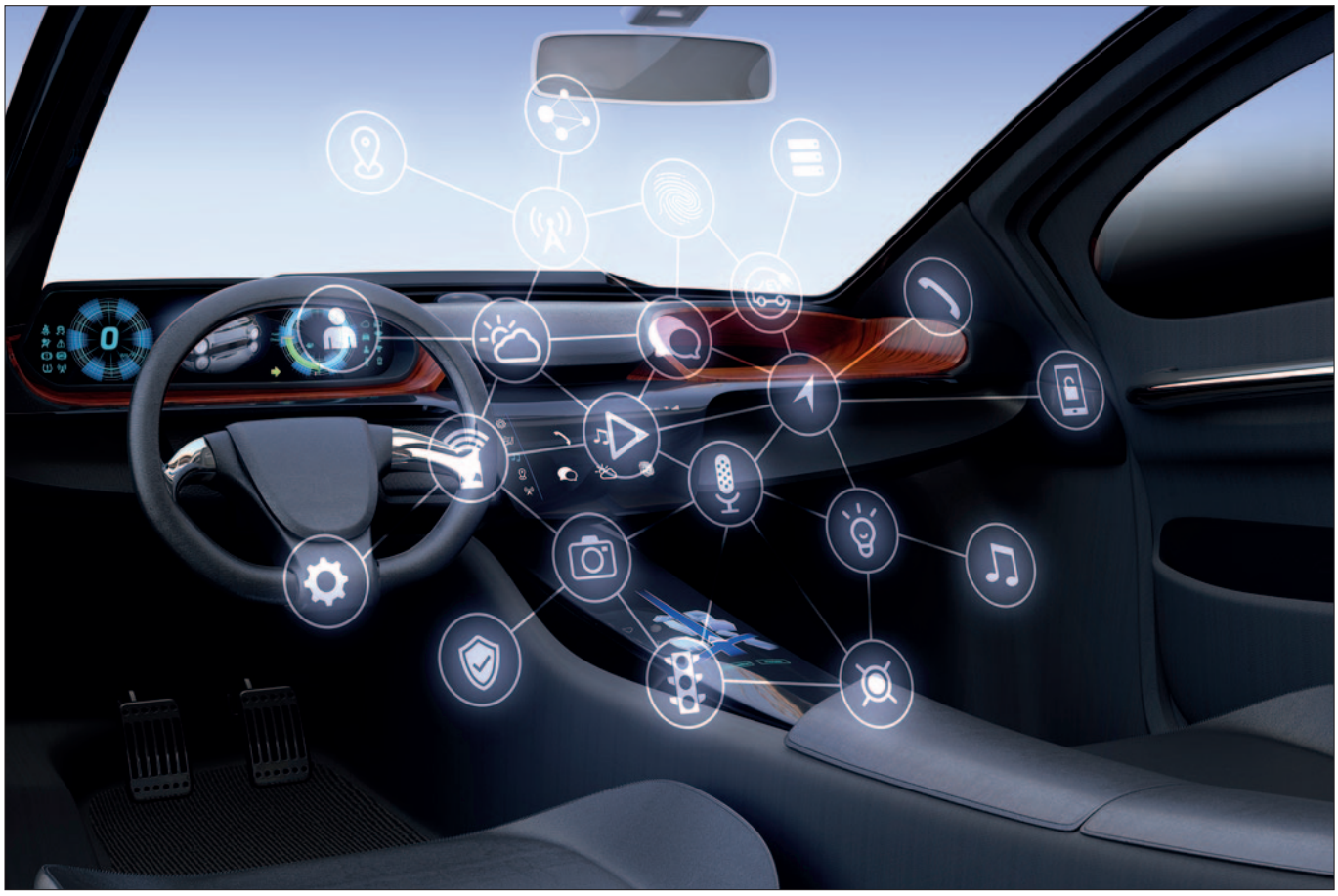


Infotainement- und Fahrassistenzsysteme sowie WLAN im Auto bieten Angriffspunkte für Kriminelle

Autodaten als Beweis

Moderne Autos sind aufgrund ihrer Elektronik und Vernetzung anfällig für Manipulationen. Sie speichern immer mehr Daten, die für kriminalpolizeiliche Ermittlungen relevant sein können.

Moderne Autos (Elektro und Verbrenner) sind aufgrund der zunehmenden Vernetzung, Digitalisierung und hochtechnologischen Ausstattung vermehrt der Gefahr von Cyber-Angriffen und elektronischen Manipulationen an Steuergeräten und Infotainment-Systemen ausgesetzt – bis hin zur Beeinflussung von Assistenzsystemen oder der Übernahme eines Fahrzeugs. Moderne Autos haben immer mehr elektronische Komponenten, die nicht nur mit der Lenkerin oder dem Lenker, sondern auch mit der Außenwelt durch eine WLAN-, Internet- oder Bluetooth-Verbindung kommunizieren können.

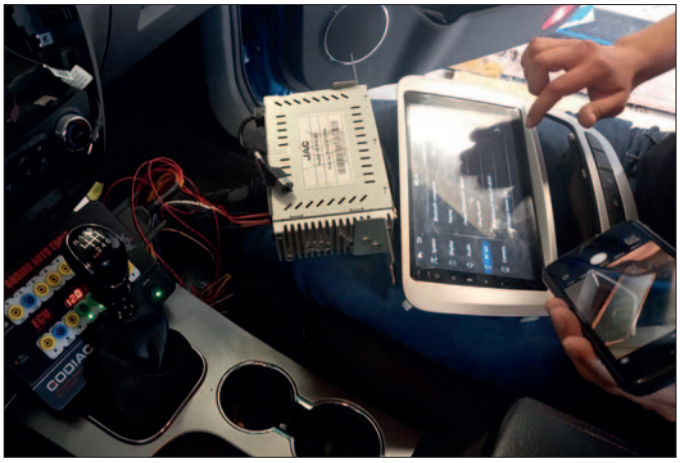
Die fortschreitende Technisierung befähigt Kriminelle, das Signal eines Transponderschlüssels („Smart Keys“) abzufangen, um sich so Zugang zum Fahrzeug zu verschaffen, beim Fahrzeug einen neuen Schlüssel zu programmieren beziehungsweise „remote“ programmieren zu lassen (Key-Learning as a Service) oder die elektronische Wegfahrsperre zu deaktivieren, um das Fahrzeug unberechtigt in Betrieb nehmen zu können.

Die Kfz-Forensik-Experten des Bundeskriminalamtes identifizierten diese neue Diebstahlsmethode (Key-Learning as a Service) und setzten Fahrzeughersteller davon in Kenntnis. Da Hersteller das Abfangen von Signalen „smarter Schlüssel“ erschwert haben und vermehrt Autobesitzer ihre Schlüssel in Metallboxen verwahren, entwickelten Kriminelle eine neue Methode, ein Auto zu stehlen, die als „CAN-Bus-Injection“ bezeichnet wird. Anstatt das Schlüsselsignal abzufangen, greifen Diebe in die interne Kommunikation des Autos – in das CAN-Bus-System – ein.

Angriffe auf den CAN-Bus. Im CAN-Bus eines Autos erfolgt der Datenaustausch zwischen Steuergeräten, Sensoren und elektronischen Modulen (CAN = Controller Area Network). Sobald der Zugriff auf den CAN-Bus gelingt, ermöglicht dies den Zugriff auf Steuergeräte, das Infotainment-System und die elektronischen Zugangs- und Sperrsysteme des Kraftfahrzeuges. Üblicherweise erfolgt der Zugriff auf die Elektronik über die OBD-Datenschnittstelle (OBD = On-Board-Diagnose), die sich zumeist im Fußraum befindet und für Service- und Wartungsarbeiten in Werkstätten vorgesehen ist.

Es kann auf den CAN-Bus auch von außen zugegriffen werden, ohne das Fahrzeug zu öffnen. Durch Demontage von Fahrzeugteilen (z. B. Scheinwerfer) gelingt der Zugriff auf die Leitungen, wobei über diese Schnittstelle mit den elektronischen Bauteilen und Steuer-

Moderne Autos lassen sich mittels einer App des Herstellers über ein Smartphone öffnen und schließen



Digitale Beweissicherung in einem Kfz: Autodaten können für kriminalpolizeiliche Ermittlungen relevant sein

geräten kommuniziert werden kann. Die Täter verwenden dafür zum Beispiel ein altes Handy, das mit einer CAN-Hardware und einer zum Auto passenden Firmware ausgestattet ist. Dabei werden die Datenkabel des CAN-Netzwerks durch die Karosserie angestochen, ein Eingabegerät (Manipulationstool) angeschlossen und Informationen an Steuergeräte gesendet, wobei die Sicherheitssysteme und die elektronische Wegfahrsperre (EWS) außer Kraft gesetzt werden können. Die Täter verschaffen sich in wenigen Minuten Zugang zum Auto. Beschädigungen am Scheinwerfer können Zeichen eines Zugriffs sein.

Diese als „Can-Bus-Injection" bezeichnete Vorgehensweise sorgt derzeit, neben den bisher bekannten Keyless-Go-Angriffen, europaweit zu steigenden Kfz-Diebstahlszahlen. CAN-Systeme sind in modernen Autos verschlüsselt. Damit wird es Dieben erschwert, mit externen Geräten das Fahrzeugsystem zu manipulieren. Ältere Modelle haben diesen Schutz nicht.

„Gameboy" als Autoöffner. Neben der „Can-Bus-Injection", wo ein physischer Zugriff auf Bauteile und Autoteile notwendig ist, tritt eine weitere Angriffsmöglichkeit in Erscheinung, die es ermöglicht, das Kraftfahrzeug zu öffnen und in Betrieb zu nehmen, ohne einen neuen Schlüssel anzulernen.

Dieses Gerät, das in einschlägigen Kreisen und auf Online-Markplätzen als „Gameboy" bezeichnet wird, ermöglicht ein kontaktloses Öffnen des Autos, indem via Funk mit der elektronischen Zutrittsberechtigung (Zentralverriegelung) kommuniziert wird und der Fahrzeugelektronik ein für dieses Fahrzeug berechtigter digitaler Fahrzeugschlüssel vorgegeben wird. Da die Elektronik einen offenbar berechtigten Schlüssel erkennt, lässt sich der Motor starten und das Fahrzeug kann wie mit dem Keyless-Originalschlüssel verwendet werden.

Fernzugriff. Durch die Nutzung von Online-Diensten und die dauerhafte Anbindung ans Mobilfunknetz und/oder WLAN (Connected Cars) ergibt sich ein zusätzliches Risiko, indem bei ungenügender Absicherung der Datenschnittstelle ein Remote-Zugriff auf das Infotainment-System, Steuergeräte oder das gesamte Kfz-System ermöglicht wird. Denkbar sind hier Zugriffe über unzureichend geschützte Bluetooth- und WLAN-Schnittstellen, Telematik-Module und Module für ein elektronisches Fahrtenbuch und Flottenmanagement. Dabei macht es keinen Unterschied mehr, ob es sich um ein Elektrofahrzeug oder ein modernes Kraftfahrzeug mit Verbrennungsmotor handelt.

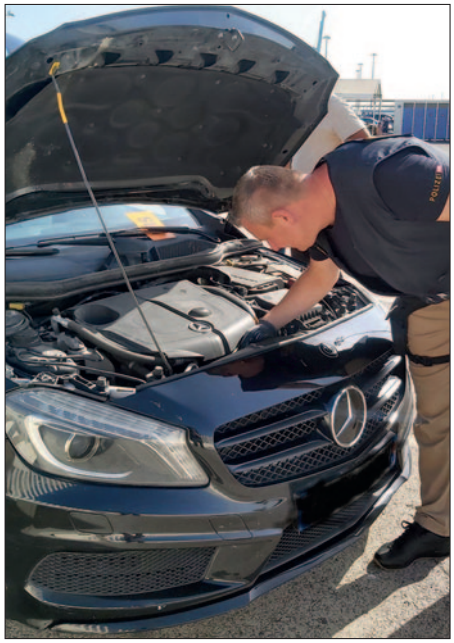
Over-the-Air-Updates (OTA-Updates) in Kraftfahrzeugen können problematisch werden, wenn der Datenaustausch nicht in einer gesicherten Form wie beispielsweise Authentifizierung, Zertifikat, Verschlüsselung oder dergleichen erfolgt. OTA-Updates dienen in der Regel für Software-Updates und Firmware-Aktualisierungen von Systemen, also

KFZ-FORENSIK/AUTOMOTIVE IT

Aufgaben

- Zentrale Ansprechstelle für Polizeidienststellen und Staatsanwaltschaften in Bezug auf digitale Beweismittelsicherung aus Kfz-Systemen.
- Bereitstellung einer operativen Einheit für Ad-hoc-Amtshandlungen, Begutachtungen und Auswertungen vor Ort.
- Unterstützung bei regionalen und überregionalen Schwerpunkten und Fahndungen bei Kfz-Diebstahl und Kfz-Verschiebung.
- Auswertung von Datenträgern und elektronischen Bauteilen aus Kfz-Systemen.
- Identifizierung von elektronischen Bauteilen und Abklärung der Historie zu den Fahrzeugdaten.
- Mitwirkung an der Tatortarbeit und ersten Ermittlungsmaßnahmen, wenn dies wegen der Straftat erforderlich erscheint, um rasch die Spurenlage festzustellen und digitale Spuren und Beweismittel gesichert werden müssen.
- Präventivmaßnahmen und Mitwirkung an der Erarbeitung von Maßnahmen zur Kriminalitätsbekämpfung. Dies umfasst auch die Kontaktaufnahme mit den Abteilungen Werkssicherheit bei den Fahrzeugherstellern, sofern eine neue Sicherheitslücke in der Elektronik und/oder ein neuer Modus Operandi bei Kfz-Diebstählen festgestellt wurde.
- Ansprechstelle für ausländische Polizeidienststellen, Europol und Interpol im Bereich Kfz-Forensik/Automotive IT sowie ständige Vertretung bei fachbezogenen Workshops, Arbeits- und Fachgruppen bei Europol und Interpol.

FOTOS: BUNDESKRIMINALAMT, ANDREY POPOV – STOCK.ADOBE.COM,



Die Spezialisten der Kfz-Forensik im Bundeskriminalamt stellen Datenträger und digitale Spuren in Autos sicher

auch Kfz-Systeme, über Funkschnittstellen wie WLAN oder Mobilfunknetz. Eine unzureichende Absicherung birgt die Gefahr, Schadsoftware oder unerwünschte Applikationen einzubringen, die Angreifern den Zugriff auf das Kfz-System ermöglichen.

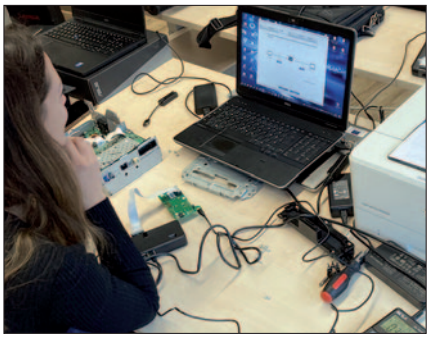
In einem Versuch der Kfz-Forensiker im Bundeskriminalamt wurde in einem einschlägigen Internet-Portal nach einem aktiven GSM/GPS-Modul gesucht, das im Flottenmanagement zur Anwendung kommt. Nachdem das für die Kommunikation verwendete Protokoll festgestellt werden konnte, erfolgte ein Verbindungsaufbau zum Modul, wobei Anfragen zu IMEI, IMSI und den aktuellen GPS-Koordinaten gestellt wurden, die auch beantwortet wurden. An dieser Stelle wurde die Kommunikation mit dem fremden Kraftfahrzeug wieder abgebrochen, da nur demonstriert werden sollte, wie rasch ein Fernzugriff auf ein Fahrzeug möglich ist.

Für weitaus mehr Aufsehen hatte der Cyber-Angriff auf *Jeeps* bereits im Jahr 2015 gezeigt, indem zwei Hacker unter Ausnützung einer Schwachstelle im Infotainment-System den Zugriff auf die gesamte Bordelektronik erlangten und einen *Jeep Cherokee* aus der Ferne mit dem Laptop steuern konnten.

Fachbereich im Bundeskriminalamt. Bei Straftaten wird oft ein Kraftfahrzeug als Transport- und/oder Tatmittel verwendet. Die Informationen, die während des Betriebes eines Kraftfahrzeuges automatisch generiert und gespeichert werden, können für kriminalpolizeiliche Ermittlungen wichtig sein.

Die Polizistinnen und Polizisten des Fachbereichs „Kfz-Forensik/Automotive IT“ im Bundeskriminalamt nehmen bundesweit gerichtsverwertbare Beweisaufnahmen vor, für alle Dienststellen des Bundesministeriums für Inneres und der Landespolizeidirektionen.

Darüber hinaus wirken die Expertinnen und Experten an Schwerpunktaktionen und operativen Einsätzen mit, wenn die sofortige Sicherung von Beweismitteln notwendig erscheint und Anordnungen der Staatsanwaltschaften vollzogen werden müssen. Der Großteil der Befundaufnahmen erfolgt am Tatort oder an Verwahrorten der Kraftfahrzeuge.



Digitale Beweissicherung nach Raubserie: Auswertung eines Kfz-Navis

„Gameboy“: Ein Tool, das ein kontaktloses Öffnen des Autos ermöglicht

Da es in Österreich keine zentrale Ansprechstelle für die digitale Beweisaufnahme an Kfz-Systemen gab, erfolgte 2014 der Antrag auf das Projekt „Fahrzeugforensik“, das über den *Fonds für Innere Sicherheit (ISF)* von der EU kofinanziert wurde. Durch die ISF-Budgetmittel konnten Arbeitsmittel und Ausrüstung gekauft werden. In weitere Folge wurde daraus ein eigener Fachbereich im Bundeskriminalamt, wo derzeit sechs Exekutivbedienstete ihren Dienst versehen. Verstärkung bekam das Team zuletzt durch eine Polizistin.

Aufgrund der stetig steigenden Anzahl an Auswertungen und unterschiedlichen Aufgaben und Teilgebiete in der Kfz-Forensik (Automotive IT) werden weitere Mitarbeiterinnen oder Mitarbeiter benötigt, die sich mit diesem Spezialgebiet der IT-Forensik befassen wollen.

Hinsichtlich vernetzter Fahrzeuge und autonomen Fahrens sowie zur Absicherung von Verkehrsleiteinrichtungen werden neue Ermittlungsmethoden und Fachkräfte erforderlich sein, um bei Straftaten die Ermittlungen und digitalen Beweissicherungen vornehmen zu können. *Horst Reisner*

FOTOS: BUNDESKRIMINALAMT, ARMIN HALM, WEST YORKSHIRE POLICE