THEMEN / WISSEN & UMWELT

SICHERHEIT

Wie leicht sich Autos hacken lassen

Einem Australier ist es jetzt gelungen, die Klimaanlage eines Nissan in England zu kapern. Die mangelhafte Sorge des Herstellers um IT-Sicherheit hat es ihm einfach gemacht. Hier lesen sie, was Hacker noch tun könnten.

Mit der Smartphone-Fernsteuerung kann der Fahrer seinen Land Rover auch einparken.

Es klingt am Anfang vielleicht noch witzig: Man sitzt am Steuer, und plötzlich macht das Auto verrückte Dinge. Die Scheibenwisch- und Waschanlage geht plötzlich an. Die Fenster öffnen und schließen sich, das Radio ändert den Kanal. Das könnte passieren, wenn ein Auto gehackt und von irgendwo auf der Welt ferngesteuert wird.

Der Australier Troy Hunt hat jetzt am Beispiel eines Nissan LEAF gezeigt, wie das geht. Er hat sich die Steuerung der Klimaanlage vorgenommen. Auch las er mit seinem Laptop Informationen über den Ladezustand der Batterie und die Fahrdaten aus: Datum, Uhrzeit und Strecke. Und das bei einem Auto, das in England fuhr, also am anderen Ende der Welt. Hacker könnten sogar noch mehr, etwa dem Fahrer die Kontrolle über Bremse, Gas und Lenkung entreißen. Und da hört der Spaß auf.

So etwas darf nicht passieren - darüber sind sich Experten aus Autoindustrie und IT-Sicherheit einig. Deshalb war Car-Hacking auch ein Thema auf der jüngsten IT-Defense - einer internationalen Fachtagung, organisiert von der IT-Sicherheitsfirma Cirosec in Mainz.

Hacker zeigen, wie es geht

Beispiele über erfolgreiche Car-Hacking-Versuche gibt es im Internet zuhauf. In einem Video überfährt eine Autofahrerin bei einem Experiment der US-Militärforschungseinrichtung DARPA eine Reihe Pylonen. Ihr letzter Bremsversuch war fehlgeschlagen. Über ihr Auto hatte die Fahrerin schon kurz zuvor die Kontrolle verloren.

Auch in anderen Kurzfilmen zeigen IT-Experten, wie sie handelsübliche Fahrzeuge per Laptop oder Mobiltelefon von außen fernsteuern - manchmal auch mit dem Willen des Autobesitzers. So ist die Fernsteuerung der Nissan-Klimaanlage durchaus im Sinne des Herstellers gewesen: Mit der App NissanConnect EV soll der Nutzer im Winter die Möglichkeit haben, das Auto vorzuheizen, zu kühlen oder den Ladezustand der Batterie abzufragen. Aber wie Troy Hunt zeigte, geht das unter Umständen auch mit Autos, die jemand anderem gehören.

Ein Auto erhält ein Software-Update. Hacker nutzen ähnliche Technik, um Autos fernzusteuern.

Beim Hersteller Land Rover können Fahrer ihre Autos mit dem Handy rangieren lassen. Steckt der Wagen in einer viel zu engen Parklücke und lässt sich die Tür nicht mehr öffnen, kann der Besitzer das Auto einfach mit seinem Smartphone ausparken - über eine Bluetooth-Verbindung. Menschen, die sich beim Ein- und Ausparken schwer tun, mag das freuen - für IT-Sicherheitsexperten ist diese Anwendung eher ein Alptraum.

DIE REDAKTION EMPFIEHLT

Wird man in der Cloud beklaut?

Häufig lagern Firmen ihre Daten nicht mehr auf der eigenen Festplatte, sondern irgendwo in der großen Welt des Internets - der virtuellen Cloud. Wie es dort mit Datensicherheit und Datenschutz aussieht, ist oft unklar. (26.02.2014)

User machen es Hackern leicht

Die automatische Notbremse für Autos setzt sich durch

Renault und Nissan setzen auf Selbstfahrautos

Autonomer LKW erstmals in freier Wildbahn

Mit dem Roboter auf der Renn-Strecke

Aus Elektronik wird Vernetzung

Im Jahr 1986 führte Bosch erstmals den CAN-Bus ein - das Controller Area Network, eine Art zentrales Nervensystem für Autos, das alle Steuergeräte miteinander vernetzt. Es verringerte die Komplexität der früher nötigen Kabelbäume drastisch und vereinfachte damit den Einbau der Komponenten.

So hielt Elektronik Einzug in die Autos und ersetzte die bis dahin übliche Elektrik. Aus dem Automechaniker wurde der Automechatroniker. Mit einem Analysegerät überprüfte er ab sofort die Funktionen aller wichtigen Bauteile: Lebenszeit, Störungen, Kilometerleistung, Ölstand und vieles mehr.

Findige Mechatroniker können seitdem mit dem Analysegerät den Tachostand um einige Zehntausend Kilometer zurücksetzen, bevor sie ein Auto weiterverkaufen. Das ist zwar verboten, aber nicht unüblich - und nachträglich nicht nachweisbar.

Wenn der Fensterheber mit der Tankdeckelentriegelung spricht

In modernen Autos steuern elektronische Controller, die ECUs, heute schon über 100 Bauteile. Im Prinzip können alle Teile über den CAN Bus oder ähnliche neuere Bus-Systeme miteinander kommunizieren.

Der CAN-Bus gilt im Sinne der Autoindustrie als sicher. Mit ihm funktionieren Airbag, Gurtstraffer, Gas und Bremse absolut zuverlässig. Praktisch gibt es keine Unfälle, die darauf zurückzuführen sind, dass dieses zentrale Nervensystem des Autos versagt. Aber sicher ist es nur deshalb, weil Automechatroniker bisher nicht versuchten, die Komponenten zu manipulieren oder zu missbrauchen. Bisher gab es auch keinen vernünftigen Grund, das zu tun.

Der Automechatroniker steuert die Funktion von über 100 Bauteilen über den Laptop.

Neue kriminelle Geschäftsmodelle

Die Autos der Vergangenheit waren in sich geschlossene Systeme: Um an der Programmierung etwas zu ändern, musste das Auto erst in die Werkstatt und ans Diagnosegerät angeschlossen werden.

Stephan Gerhager ist bei der Allianz Versicherung für IT-Sicherheit zuständig.

Das Auto von heute ist aber völlig anders, sagt Stephan Gerhager, IT-Sicherheitschef bei der Allianz-Versicherung. "Die größten Schwächen bei den Fahrzeugen liegen in der zunehmenden Vernetzung. So treffen Viren und Trojaner plötzlich auf Fahrzeuge, die eine deutlich höhere Sensibilität an Funktionen im Inneren des Fahrzeugs haben."

Das Auto von heute gleicht laut Gerhager eher einem Computer oder einem Mobiltelefon auf Rädern. Aber es gebe einen wichtigen Unterschied: "Wenn beim Kunden der Internetfernseher oder der Computer ausfällt, ist das nicht lebensbedrohlich." Die Vernetzung öffnet neuen kriminellen Geschäftsmodellen Tür und Tor. Ein Diebstahl ohne Gewaltanwendung ist dabei vielleicht noch eins der harmloseren Szenarien.

Gerhager meint, dass die Autoindustrie Sicherheit im Automobilbereich nochmal ganz neu erfinden müsse: "Die innere Vernetzung im Fahrzeug hat sich in den letzten Jahren nicht verändert. Die Funktionen sind exakt genauso implementiert wie schon vor 15 Jahren." Die Ingenieure sollten jetzt von den Erfahrungen der IT aus den letzten Jahrzehnten lernen und die Fehler der Computerentwickler nicht wiederholen.

Für jeden Rückspiegel ein eigenes Passwort?

Der Fall Nissan zeigt, wie einfach es die klassische Autoindustrie Hackern macht: Die Prinzipien der IT-Sicherheit hat sie offensichtlich nicht verinnerlicht. So ist das Zugangspasswort für die NissanConnect App identisch mit der Identifikationsnummer des Fahrzeugs - und die ist mit einem Barcode an der Windschutzscheibe angebracht. Das ist zwar praktisch für Autovermietungen, die per Lesegerät die Fahrzeuge schnell und unproblematisch registrieren, widerspricht aber allen Prinzipien von IT-Sicherheit.

Wenn das Auto immer mehr zum Computer wird, werden sich die Kunden wohl bald darauf einrichten müssen, dass sie ihre Autos wie Computer behandeln müssen. Heute ist es selbstverständlich, Betriebssystem, Browser, Firewall und Virenprogramme regelmäßig upzudaten und Back-ups anzulegen. Aber hat sich schon mal jemand Gedanken darüber gemacht, ob die Firmware des eigenen Autos noch auf dem aktuellen Stand ist? Wer kennt schon die Passwörter für einzelne Komponenten des Fahrzeugs - so es sie denn überhaupt gibt? Und müssten die nicht auch sicherheitshalber regelmäßig gewechselt werden?

Oldtimer sammeln ist out! Ohne Firmware-Updates sind alte Autos in Zukunft vielleicht nur noch Elektroschrott.

Für all diejenigen, die in dreißig Jahren noch einen Oldtimer fahren wollen, stellt sich vielleicht irgendwann folgende Frage: Ab wann stellt mein Hersteller den Software-Support für meinen Wagen ein?

WWW-LINKS