Veröffentlicht auf *LANline* (http://www.lanline.de)

Autobauer haben IT-Sicherheit verschlafen

IT-Defense, Mainz
Autobauer haben IT-Sicherheit verschlafen
geschrieben von LANline/Dr. Wilhelm Greiner am 28.01.2016

Auf der von Cirosec ausgerichteten Sicherheitskonferenz IT-Defense in Mainz diskutierte Stephan Gerhager, CISO der Allianz, die Angriffsmöglichkeiten auf vernetze Fahrzeuge. Er zeichnete ein recht bedrohliches Bild - selbst für deutsche Hersteller.

Ein heutiger Pkw beinhaltet laut Stephan Gerhager über 100 ECUs (Electronic Control Units), in neuesten Fahrzeugen finde man noch deutlich mehr. Funktionen wie Parkassistenten erforderten dabei die Echtzeitkommunikation zwischen ECUs über interne Bussysteme wie CANbus.

Der Wunsch nach Remote-Funktionalität wie etwa das Betätigen der Hupe per App zum leichteren Finden des Fahrzeugs setzt zudem eine Anbindung ans Internet voraus. Die Folge, wie 2015 der Jeep-Cherokee-Hack von Charlie Miller und Chris Valasek verdeutlichte: Die komplette Übernahme eines modernen Autos durch einen Angreifer ist nicht nur per Diagnose-Port, sondern auch via Internet möglich. Gerhager zeigte dazu ein kurzes Video, in dem Dan Kaufman von der US-Behörde Darpa (Defense Advanced Research Projects Agency) einen solchen Angriff demonstrierte (auf Youtube zu finden unter www.youtube.com/watch?v=7E1WsdODxu0).

Das Problem laut Gerhager: Die Mitarbeiter eines Automobilkonzerns, die von IT-Sicherheit Ahnung haben, sitzen in der IT des Herstellers, nicht in deren Entwicklungsabteilung. „Jetzt machen die [die Entwickler, d.Red.] dieselben Fehler, die wir in der IT vor zehn, 15 Jahren gemacht haben“, warnt der Allianz-CISO.

Jede Fahrzeugserie hat laut Gerhager heutzutage ihre eigene IT-Architektur, die es zuerst per Sniffing zu ermitteln gelte. Dies sei dank aktueller Linux-Tools wie CANtact kein Problem mehr. Nach einem Tag Arbeit habe ein (allerdings in Autotechnik sehr versierter) Praktikant in Gerhagers Haus einen erfolgreichen Angriff von innerhalb des Fahrzeugs durchführen können.

Laut dem Allianz-Mann waren die zwölf Angriffe, die Charlie MIller und Chris Valasek letztes

Jahr erfolgreich und spektakulär gegen einen Jeep Cherokee durchgeführt haben (LANline berichtete), bei deutschen Herstellern überwiegend erfolglos, dank Maßnahmen wie Netzwerksegmentierung, die der Cherokee nicht bot.

Nach internen Angriffen die nächste Stufe: ein Angriff an der Außenhaut des Fahrzeugs - Einfallstore könnten hier Bluetooth sein, WLAN/Remote Key oder auch das Reifendruck-Kontrollsystem. Ein Angriffer könne sich zum Beispiel bei einem Remote Key per Man-in-the-Middle-Angriff zwischenschalten und so das Verschließen des Fahrzeugs verhindern. Nach einem Diebstahl könne der Angreifer je nach Hersteller das Fahrzeug sogar wieder unbemerkt zusperren - im Diebstahlsfall ein Problem für den Inhaber wie den Versicherer: Wie weist der Fahrer nach, dass ein Einbruch erfolgte?

Der anspruchsvollste Angriff ist, wie jener von Miller und Valasek, ein Remote-Zugriff auf die Steuerungselektronik des Fahrzeugs. Per Reverse Engineering können Angreifer dann die Fahrzeugsoftware manipulieren. Für den Fernzugriff benötigt man laut Gerhager ein fest vorgegebenes Challenge (Seed). Dies könnte zum Beispiel der Herstellungszeitpunkt sein - der allerdings mitunter, je nach Hersteller, der Fahrgestellnummer zu entnehmen sei. In der Firmware der Fahrzeuge finde man zudem zahlreiche Angaben, die Angreifern wichtige Hinweise für ihr weiteres Vorgehen geben können, warnt der Allianz-Mann.

Gerhagers Fazit: Die Autohersteller - auch die deutschen - hätten wichtige Entwicklungen der IT-Sicherheit „verschlafen“, ihre Lernkurve beim Thema IoT-Sicherheit gehe jetzt erst los. Die Autobauer setzten auf den unsicheren CANbus, und durch das Öffnen der Fahrzeuge zum Internet seien die Fahrzeuge kompromittierbar. Für Spezialisten - wie es sie zum Beispiel im Umfeld des Chip-Tunings gebe - stehe damit das Tor für Kompromittierungen offen. Neben Autodiebstahl seien sowohl gezielte Angriffe als auch Erpressungen der Fahrzeughersteller denkbar.

Eine Pointe am Rande: Die Diebstahlsquote für Land Rover liegt dramatisch höher als bei anderen Fahrzeugen - nicht nur, so Gerhager, weil der teure Geländewagen sehr beliebt sei, sondern auch, weil er lange eine sehr schlechte Diebstahlsicherung aufgewiesen habe. Land Rover habe einerseits mit einer neuen Schlüsselgerneration reagiert, andererseits durch eine firmeneigene - kostengünstige - Diebstahlversicherung, mit der Land Rover die Schwächen des Fahrzeugs „subventioniere“. Deshalb sei er als Allianz-Mann und Land-Rover-Fahrer jetzt bei Land Rover versichert: Die Versicherungsprämie sei sonst „nicht mehr darstellbar“.

Weitere Informationen zur IT-Defense finden sich unter www.it-defense.de.

Mehr zum Thema:

IT-Defense, Mainz: Hacken mit Bildern

Black Hat und Def Con, Las Vegas: Nichts ist sicher