Die Auto-Industrie muss Cyber-Security

In Werbe-Spots übertreffen sich die Autobauer gegenseitig, wenn es um die Schlagworte Digitalisierung, Connected Car und Internet geht. Bei der Cyber-Security fahren sie anderen Branchen um Jahrzehnte hinterher. Das zeigen die großen Sicherheitslücken, etwa bei Funkschlüsseln, die nur mit einer äußerst simplen Kryptographie abgesichert sind. Dabei ist weit entwickelte Verschlüsselungstechnologie etwa im Banking-Bereich heute bei jeder ländlichen Raiffeisenbank Alltagsgeschäft. Die Autoindustrie geht damit das große Risiko ein, wichtiges Vertrauen insbesondere beim großen Thema automatisiertes Fahren zu verlieren.

stärker auf achten

PROF. DR. FERDINAND DUDENHÖFFER,
Direktor des CAR-Center Automotive Research an der Universität Duisburg-Essen sowie Inhaber des Lehrstuhls für Allgemeine Betriebswirtschaftslehre und Automobilwirtschaft an der Universität Duisburg-Essen.

Gegen Cyber-Angriffe ungeschützte oder nur unvollständig geschützte Autos können deutlich mehr Schaden anrichten, als einfach das Türschloss zu knacken. Das hat 2015 der Hack des Jeep Cherokee gezeigt. Den US-Hackern Miller und Valasek war es gelungen, einen Jeep Cherokee wären der Fahrt zu „hacken" und etwa mitten auf einem Highway ferngesteuert zum Stehen zu bringen. Die Auto-Industrie muss sich schneller und stärker um das Thema Cyber-Security kümmern. Millionen Funkfernbedienungen wurden von den Autobauern mit ein und demselben Passwort „abgesichert". Das ist fast so, als würde man sein Passwort auf einer Website publizieren. Um das Bedrohungspotenzial für unsere neue, vernetzte Mobilitätswelt abzusichern, müssen Regeln beachtet werden. Am CAR-Institut der Universität Duisburg-Essen haben wir dazu sieben Grundsätze zusammengefasst.

REGEL 1: Jede nicht triviale Software hat Bugs, also Fehler – ein absoluter Schutz existiert nicht.

Dringt ein Fremder in die Software eines Rechners im Auto ein, kann er den Rechner dazu bringen, beliebige Kommandos auszuführen, sprich, Fehler zu erzeugen. Die Informatiker sagen da gerne „Bug", sprich Käfer, dazu. Dies ist ähnlich zu einem Virus auf einem PC. Eine Art Gesetz der Informatik lautet: Jede nicht triviale Software hat Bugs. Damit ist es theoretisch möglich, auch jede Software in einem Auto zu knacken. „Hört auf zu sagen, dass eure Autos nicht hackbar sind. Das ist lächerlich", hatte der Jeep Cherokee Hacker Chris Valasek als Botschaft an die Adresse der Autobauer gerichtet. Nach der Regel 1 hat er Recht. Eine alte Faustregel unter Software-Entwicklern besagt, dass bei 1000 Zeilen handgeschriebener Codes im Durchschnitt sich ein Programmierfehler einschleicht. Die Software in unseren Autos hat mehrere Millionen Zeichen und die Zeichenzahl steigt mit neuen Funktionen im Auto fast schon mit Schallgeschwindigkeit. Eine Zukunft mit absoluter Hacker-Sicherheit ist unmöglich.

REGEL 2: Software im Auto und damit das Hacking-Risiko nehmen in hohem Tempo zu.

Entertainment-Systeme, Fahrerassistenzsysteme, teilautonomes Fahren, autonomes Fahren sind wichtige Entwicklungen für unsere Autos. Komfort – aber wesentlich wichtiger – die Sicherheit des Straßenverkehrs nimmt durch den Übergang zum autonomen Fahren exponenziell zu. Es wäre also falsch, darauf zu verzichten. Mit dem Wachstum der Software im Auto steigt das Hacking-Risiko. Die Autobauer müssen also schnell und umfassend Sicherheitssysteme aufbauen.

REGEL 3: Die Trennung vom Infotainment-System und sicherheitskritischen Steuergeräten ist nur die „halbe Miete".

Natürlich könnte man daran denken, die Sicherheits- und Infotainment-Systeme strikt als getrennte Systeme zu behandeln. Auto-Software wird erst angreifbar, sobald sie über ein Netzwerk angesprochen wird. Um Cloud-Services (Musik, Navigation etc.) zu nutzen, wird das auch so vom Kunden gefordert. Das bedeutet wiederum, dass ein Auto eine IP-Adresse erhält, was wiederum bedeutet, dass jeder

dem Auto IPPakete (Datenpakete) senden kann. Wenn diese Systeme physikalisch getrennt sind, dann kann ein Hack des Infotainments unmöglich in die Motorsteuerung eingreifen, weil diese keinerlei Daten miteinander austauschen. Das wird aber bei dem Weg zum teilautonomen und autonomen Fahren nicht machbar sein. So greift etwa das Google-Betriebssystem Android-Auto auf das GPS und die Radsensoren zu, um eine präzisere Lokalisierung des Autos, etwa in einem Tunnel, zu erhalten. Unsere Autos sollen miteinander kommunizieren, um etwa eine Notbremsung automatisch auslösen zu können. Dies sind nur einige Beispiele, die zeigen, dass eine Trennung zwischen Infotainment und Sicherheitssystemen nur die halbe Miete wäre, denn die sicherheitsrelevanten Rechner in unserem Auto brauchen Information von draußen, sprich, von einem Netzwerk. Damit sind sie nach Regel 1 hackbar. Zum Zweiten stellt sich die Frage, was eigentlich sicherheitsrelevant ist. Wenn plötzlich das Radio auf voller Lautstärke aufdreht, die Türverriegelung während der Fahrt anfängt „verrückt" zu spielen, Fenster und Schiebedach sich automatisch öffnen, die Cockpit-Anzeigen „durchdrehen", die Klimaanlage Wüstenhitze erzeugt, und, und, und … Es gibt also nur einen unvollständigen Schutz.

REGEL 4: Schutzräume durch Sand-Boxing-Verfahren aufbauen.

Bei modernen Web-Browsern wird zum Hackerschutz das sogenannte Sand-Boxing-Verfahren genutzt. Mit anderen Worten, es werden mehrere Sicherheitsbarrieren errichtet. Fällt die erste, hat der Hacker nur Zugriff auf die Sand-Box, welche nur beschränkte Rechte hat. Er braucht dann einen weiteren Hack, um aus der Sand-Box auszubrechen und seine Rechte auszuweiten. Auch das ist möglich, es ist aber eben weit weniger wahrscheinlich. Hier muss die Auto-Industrie noch mehr darüber lernen wie professionelle Software-Entwickler aus der Internet-Industrie heute arbeiten.

REGEL 5: Jede Software muss mit Updates versorgt werden – das muss auch für Autos gelten.

Microsoft und andere Software-Unternehmen bieten permanent Updates für ihre Programme. Ein Hauptgrund für diese Updates sind bekannt gewordene Sicherheitslücken. Wenn man so will, spielen Hacker und Software-Hersteller permanent Katz und Maus. Nach Regel 1 endet das Spiel praktisch nie. Sobald eine Lücke geschlossen wird, suchen die Hacker die Neue. Der gängigste Sicherheitsfehler ist, dass die aktuelle Software die erhaltenen Daten nicht rigoros überprüft, sondern gutgläubig benutzt. Das führt zum Fehlverhalten der Software. Es werden also Fehler in der Programmierung ausgenutzt. Die meisten Hacker nutzen üblicherweise diese Sicherheitsfehler aus und manipulieren so die Software.

REGEL 6: Jede Software ausgiebig testen und Hacker-Abteilung einrichten.

Die Hersteller müssen ihre Software also sehr genau testen und von Hackern überprüfen lassen, die im Rahmen von Penetrationtests versuchen, Fehler zu finden. Nur so können diese Lücken geschlossen werden, bevor die Software zum Kunden kommt. BMW hatte beispielsweise bei seinen mit dem Connected-Drive-System ausgerüsteten Modellen vergessen, die Verschlüsselung einzuschalten, weswegen man einen BMW per Netzwerk aufsperren konnte. Bei dem Jeep-Cherokee-Hack handelte es sich auch um Programmierfehler im Infotainment-System. Dass man hier auch unkonventionell vorgehen kann, hat Elon Musk, der Tesla-Gründer, bewiesen.

Das Modell Tesla S hat ein sehr breites und großes Software-System. Für jeden Hacker ist es eine Herausforderung, den Software-Benchmark der Auto-Industrie zu hacken. Musk hat einfach einen Wettbewerb ausgeschrieben und dann die besten Hacker bei Tesla eingestellt. Autobauer und Zulieferer brauchen also eine eigene Hacker-Abteilung.

REGEL 7: Verschlüsselungs-Technologien weiterentwickeln.

Die einfachen Hacks sind Zugriffe aufgrund von Programmfehlern. Anspruchsvoll wird es, wenn man den Verschlüsselungs-Code knacken kann. Man kann das ein bisschen mit der Enigma, der Verschlüsselungsmaschine der deutschen Geheimdienste im Dritten Reich, vergleichen. Die Enigma galt lange Zeit als „unknackbar", bis der Code eben dann doch durch erheblichen mathematischen Aufwand entschlüsselt wurde.

Das Modell Tesla S hat ein sehr breites und großes Software-System. Für jeden Hacker ist es eine Herausforderung, den Software-Benchmark der Autoindustrie zu hacken.

Von da an konnten die Alliierten den gesamten deutschen verschlüsselten Funkverkehr abhören, wussten also, was der Gegner plante. In der Mathematik ist die Kryptographie eine Spezialdisziplin, die sich mit Verschlüsslung von Daten beschäftigt.

Für anspruchsvolle Hacker ist es also denkbar, nicht Programmierfehlern hinterherzujagen, sondern den Verschlüsselungs-Code zu knacken. Hat man das geschafft, kann man beliebig in die Software eingreifen. Mathematisch ist das sehr anspruchsvoll und kommt eher selten vor. Wozu sich mit „Mathe“ quälen, wenn man auch Programmierfehler nutzen kann, die nach Regel 1 immer existieren werden.

Zusammenfassend gilt: Es gibt keinen absoluten Schutz gegen Cyber-Crime, aber es gibt Vorkehrungen, die das Hacking-Risiko deutlich minimieren. In der Auto-Industrie sind diese Vorkehrungen nur wenig ausgepägt. Einfach, weil man die Probleme in der Vergangenheit nicht gesehen hat. Bisher waren die Autobauer zu „blauäugig“ gegenüber Hacking und unsere europäischen Gesetzgeber eher blind. Es spricht viel dafür, dass das Hacken von Autos für Kriminelle ein lukratives Aktionsfeld wird.

Terroristische Anschläge kann man zwar genauso wenig ausschließen wie Taten von psychologisch Gestörten. Die überwiegenden Tatmotive werden aber, wie etwa beim Cyber-Crime im Online-Banking, von der kriminellen Geldbeschaffung ausgehen.

Beispielsweise befallen Lösegeld-Viren (Ransomware) heute fast ausschließlich PCs und Notebooks. Erst wenn der Geschädigte Geld – etwa Bitcoins – auf ein anonymes Konto überweist, wird der Zugriff auf die Festplatte des PC wieder freigeschaltet. Was würden Sie tun, falls Ihr Wagen des Nachts auf einer abgelegenen Straße stillgelegt wird und Sie eine Zahlungsaufforderung per SMS bekommen? Sofern die geforderte Summe nicht zu hoch ist, werden Sie wahrscheinlich zahlen.

von Prof. Dr. Ferdinand Dudenhöffer