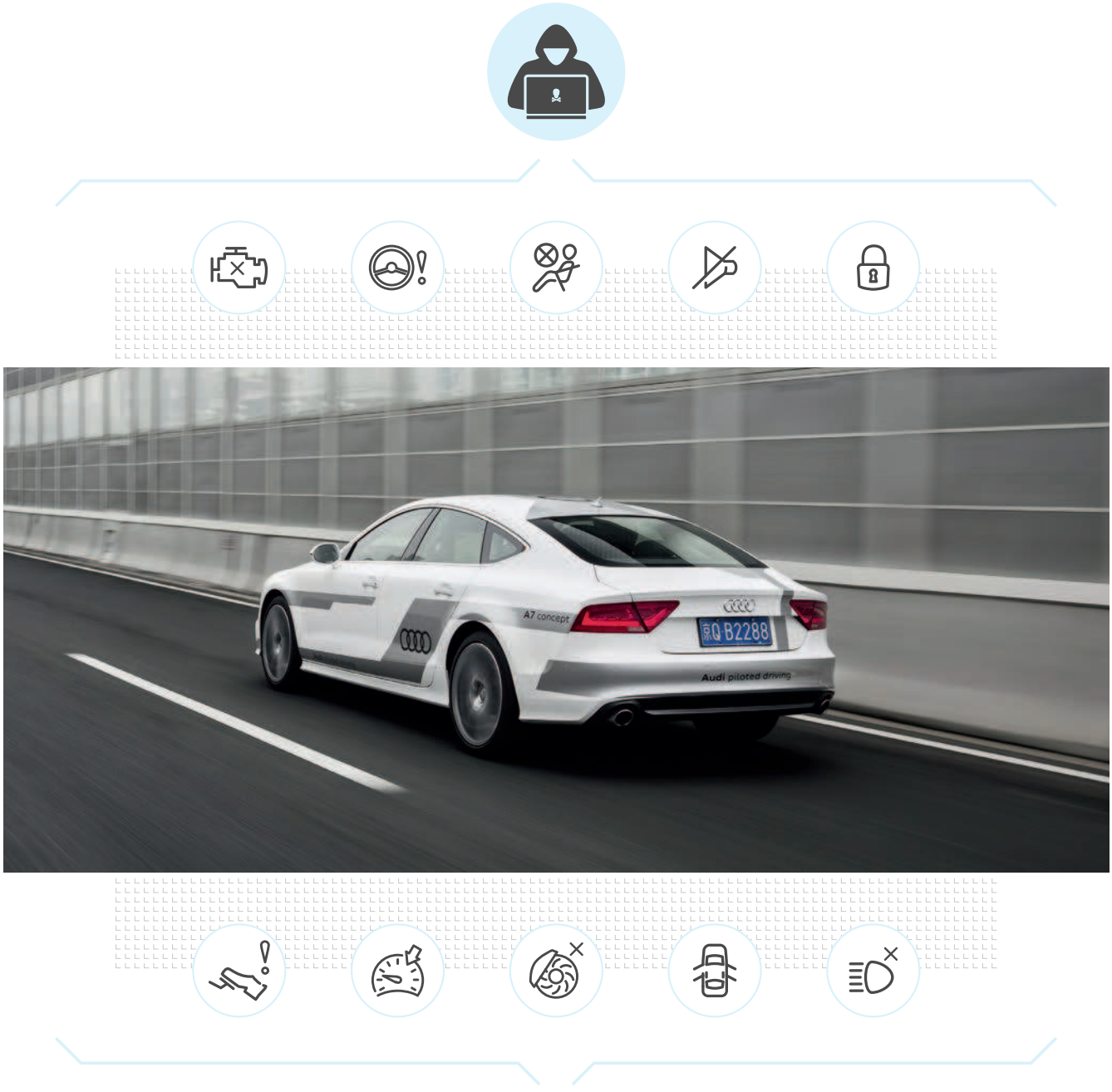
Rollende Sicherheitslücken

Die Automobilbranche vernetzt neue Modelle auf Teufel komm raus. Kritischen Fragen zur **Sicherheit von Bordsystemen, Apps und Nutzerdaten** aber gehen die Hersteller geflissentlich aus dem Weg.



Kriminelle Hacker verschaffen sich Zugriff auf die vernetzten Fahrzeugsysteme und können Autos ferngesteuert stehlen oder gegen einen Baum fahren lassen – ein Horrorszenario für die Autoindustrie. Tatsächlich kann es Realität werden. Denn mit der Vernetzung der Systeme wächst die Zahl der Angriffsflächen. Hackern ist es bereits mehrfach gelungen, in Fahrzeugsysteme einzudringen und damit für viel Aufsehen in der Fachwelt zu sorgen. Als Gegenspieler für die Hersteller agieren keine Scriptkiddies, sondern die organisierte Kriminalität. Die professionelle Erpressung von Autokonzernen kann sich zu einem höchst lukrativen Geschäftsfeld entwickeln. Die hinter verschlossenen Konzerntüren – aber auch verstärkt in der Öffentlichkeit – heiß diskutierte Gretchenfrage lautet: Wie sicher sind das vernetzte Auto und seine Daten tatsächlich? Fachleute für IT-Sicherheit sind in den technischen Details unterschiedlicher Meinung, identifizieren aber mehrere Schwachstellen. „Ein großes Problem ist die fehlende Netzwerktrennung zwischen der Fahrzeugsteuerung und dem Entertainment. Sie ist noch längst nicht überall vollzogen“, sagte zum Beispiel Martin Wundram, Geschäftsführer von DigiTrace. Er macht Penetrationstests von Bordelektronik, Multimedia und Backend und berät einen Hersteller in der IT-Sicherheit. Die Autobauer trennen zwar die Netze zu einem gewissen Grad, Hacker konnten das aber überwinden. „Eine strikte Trennung wird man nicht immer durchhalten können, denn für viele Funktionen muss das Infotainment auf Sensoren zugreifen. Gegen dieses Problem gibt es kein Patentrezept“, bestätigt Christian Wieschebrink vom Referat Cybersicherheit für die Digitalisierung in Verkehr und Industrie 4.0 im Bundesamt für Sicherheit in der Informationstechnik (BSI).

Schwierig gestaltet sich auch die dringend erforderliche Zusammenarbeit zwischen Ingenieuren und IT-Sicherheitsexperten. In der neuen Vernetzungswelt müssen sich plötzlich Menschen interdisziplinär austauschen und zusammenarbeiten, die im Autobau früher nichts miteinander zu tun hatten. Da treffen völlig unterschiedliche Herangehensweisen und Ausbildungsrichtungen aufeinander. Das Thema Kooperation ist auch in der Lieferkette ein entscheidender Knackpunkt, denn die Hersteller müssen Fremdkomponenten und die Produkte ihrer Zulieferer auf Sicherheit prüfen. Transparenz und Offenheit ist auch bei Sicherheitsvorfällen gefragt, wenn polizeiliche Ermittler und Sachverständige Einblick in die elektronischen Systeme bekommen. „Die Hersteller sind dazu nicht verpflichtet“, so Wundram. Er fordert analog zu Flugzeugen eine Blackbox, die nach einem Unfall ausgewertet werden kann. Der Gesetzentwurf zum automatisierten Fahren sieht einen solchen Speicher vor. Ein weiterer Problembereich ist der Datenschutz: „Ein besserer Datenschutz würde die Sicherheit erhöhen. Die Hersteller sollten Respekt haben vor den Daten ihrer Kunden“, sagt DigiTrace-Geschäftsführer Martin Wundram. Als riskant für die Privatsphäre gilt zum Beispiel der digitale Assistent Alexa von Amazon. Seit Herbst 2016 integriert BMW seinen personalisierten Mobilitätsassistenten BMW Connected in Alexa und Alexa-fähige Endgeräte. Dennoch kommt Martin Krauss, als Direktor bei CA für den Geschäftsbereich Sicherheit in Europa verantwortlich, zu einer positiven Gesamteinschätzung. CA arbeitet mit VW, Daimler und BMW zusammen. „Die Daten sind sicher, denn sie werden verschlüsselt abgelegt und kommuniziert.“ Wieschebrink schränkt diese Aussage ein: „Kryptoverfahren müssen richtig implementiert werden. Die Systeme müssen so flexibel sein, dass die Verfahren ausgetauscht und Updates aufgespielt werden können.“ Angesichts der langen Lebensdauer von Autos ist das ein Muss. Eine wichtige Grundlage für digitale Sicherheit liefert das Prinzip „security by design“, bei dem Entwickler Sicherheitsaspekte von Anfang an mitdenken müssen. Nach Meinung von

Good to know

Leaks bedrohen autonomes Fahren

Auf den ersten Blick sind die von Wikileaks Anfang März veröffentlichten CIA-Praktiken nur eine weitere Enthüllung im Stil Edward Snowdens. Doch Sicherheitsexperten schätzen die Sprengkraft der geleakten Dokumente als deutlich brisanter ein. Durch die bekannt gewordenen Angriffstechniken der CIA droht nicht nur politischer Schaden. Für Kriminelle lesen sich die teilweise mit Code veröffentlichten Dateien wie Do-it-yourself-Anleitungen. Sie stellen ernste Sicherheitsrisiken dar. Die häppchenweise herausgegebenen Infos können eine Vielzahl von Angriffsoptionen liefern, zum Beispiel auf Betriebssysteme und Hinweise auf Anfälligkeiten bei iPhones und Android-Smartphones. Experte Sandro Gaycken von der European School of Management and Technology in Berlin schätzt, dass mehrere Millionen Zeilen Code offengelegt werden. Zwar relativiert der Programmierer-News-Dienst „Heise Online“ diese Einschätzung. Dennoch könnte es heikel werden: Auch eingebettete (embedded) Systeme wurden vom Geheimdienst unterwandert. 2014 hat die CIA den Enthüllungen zufolge dafür extra einen Bereich aufgebaut. Eingebettete Systeme in Autos, Flugzeugen oder Kraftwerken bieten eine beträchtliche Angriffsfläche. Die Automobilindustrie könnte es besonders hart treffen. Das Zukunftsthema autonomes Fahren ist gesellschaftlich weiterhin umstritten, die Angst vor Hacks groß. „Innovationen in den Feldern Smart Car oder Industrie 4.0 könnten mit den Leaks um Monate zurückgeworfen werden, wenn nicht Jahre“, schätzt Gaycken. Schließlich müssten sich Zulassungsbehörden und Versicherer damit intensiv auseinandersetzen.

Fotos: Audi, Shutterstock/iconstock, Shutterstock/Yury Vainitski

Der Schutz des Fahrzeugs vor Hackerangriffen wird gerade im Zeitalter des autonomen Fahrens immer relevanter

Krauss wird die Automobilindustrie diesem Ansatz durchaus gerecht, da sie in weiten Teilen eine Multi-Faktor-Authentifizierung einsetzt. Wieschebrink urteilt differenziert: „Security by Design ist nötig, da viele drahtlose Schnittstellen abgesichert werden müssen, zum Beispiel Mobilfunk, Bluetooth oder WLAN. Bei der Car-to-Car-Kommunikation wurde die Sicherheit im Grundsatz schon im Frühstadium berücksichtigt.“ Technische Details ihrer Systeme aber halten die Hersteller vor dem BSI zurück.

Ein mögliches Einfallstor bei Angriffen sind mobile Apps. Mit ihnen lassen sich Standortkoordinaten und die zurückgelegte Route von Autos ermitteln, Türen öffnen, der Motor starten und im Fahrzeug befindliche Geräte kontrollieren. Kaspersky Lab

Kommentar

Ulrich Hottelet
Autor

Wegducken hilft nicht

Wenn sich ein Journalist mit Fragen zu IT-Sicherheit und Datenschutz an die Pressestellen der deutschen Autohersteller wendet, trifft er auf wenig Auskunftsbereitschaft. Die VW-Pressestelle zum Beispiel ignorierte schlicht und einfach gleich mehrere Anfragen von carIT. Etwas professioneller agierten Daimler und BMW: Gespräche mit IT-Sicherheitsexperten, in denen die diversen Schwachstellen hätten beleuchtet werden können, wurden zwar auch in Stuttgart und München abgelehnt. Immerhin aber erhielt die Redaktion schriftliche Stellungnahmen. Die aber stellten sich als nichtssagend und vage heraus. Einen näheren Einblick in die sensible Problematik wollen die OEMs offensichtlich nicht gewähren. Klar, IT-Sicherheit und Datenschutz gehören nicht zu den Gewinnerthemen in der Autobranche. Damit kann man bei potenziellen Käufern nicht so gut punkten wie mit schnittigem Karosseriedesign und Fahrkomfort. Doch darauf zu hoffen, dass sich Kunden auch in Zukunft nur für die Verkaufsargumente der Vergangenheit interessieren, ist blauäugig. Die Kundschaft wird Auskunft verlangen, was mit ihren Daten geschieht. Ob die Autobauer künftig jederzeit wissen, wo ihre Fahrzeuge gerade fahren oder parken und ob sie garantiert davor geschützt sind, dass kriminelle Hacker sie ferngesteuert gegen einen Baum lenken. Der Eindruck drängt sich auf, dass VW, Daimler und BMW keine befriedigenden Antworten auf diese essenziellen Fragen geben können. Mit einer solchen Vogel-Strauß-Politik lassen sich Journalisten eine Zeitlang abwimmeln. Die Käufer aber werden diese Intransparenz der Industrie auf lange Sicht nicht durchgehen lassen.

hat sieben Apps von Herstellern zur Fernsteuerung von Fahrzeugen in einer Studie untersucht. Laut der Statistik von Google Play wurden die Apps zehntausendfach heruntergeladen, in einigen Fällen überschritten die Downloads sogar die Fünfmillionenmarke. Bei allen Anwendungen zeigten sich verschiedene Sicherheitslücken. Kaspersky kritisierte unter anderem den mangelnden Schutz vor Reverse Engineering, das Angreifer in die Lage versetzt, Schwachstellen zu identifizieren. Außerdem konnten Programme überschrieben werden, bei der Anzeige in Fenstern drohte Phishing-Gefahr und das Speichern von Nutzernamen und Passwörtern erfolgte im Klartext, was sie leicht auslesbar machte. Dadurch könnten Hacker die Kontrolle über das Fahrzeug erlangen, die Türen öffnen, den Alarm ausschalten und den Pkw stehlen. Zwar müssten Cyberkriminelle zuvor Autofahrer dazu bringen, eine schädliche App auf ihrem Gerät zu installieren. Das aber gelingt mit Social-Engineering-Tricks, die in der Szene zum Standardrepertoire gehören. „Als wichtigstes Ergebnis unserer Untersuchung können wir festhalten, dass derzeit Fahrzeug-Apps noch nicht hinreichend gegen Angriffe durch Malware geschützt sind. Es reicht nicht aus, nur die Server-seitige Infrastruktur abzusichern. Wir erwarten, dass die Autoindustrie den gleichen Weg gehen wird wie die Banken bei ihren ersten Finanz-Apps. Diese waren anfänglich auch mit Risiken behaftet. Viele Banken haben dann nach zahlreichen Sicherheitsvorfällen den Schutz ihrer Finanz-Apps verbessert. Glücklicherweise gab es bislang noch keine Angriffe auf Fahrzeug-Apps“, sagt Victor Chebyshev, Sicherheitsexperte bei Kaspersky Lab. Ins gleiche Horn stößt Martin Wundram: „Besonders wenn Fahrzeuge mit Apps vernetzt werden, zum Beispiel zur Lokalisierung, ist ein unberechtigter Zugriff möglich. Die Apps und Serversysteme der Hersteller sind unsicher programmiert.“ CA-Mann Krauss sieht das vernetzte Auto gar als „Smartphone mit Rädern dran“, denn die Autobauer wollen möglichst viel Komfort bieten. Wenn man bedenkt, wie leicht echte Smartphones inzwischen mit Schadsoftware infiziert werden können, wird das große Gefahrenpotenzial deutlich. Die IT-Sicherheit des Autos hängt entscheidend auch von der Sicherheit des Smartphones ab.

carIT wollte diese Vielzahl von Schwachstellen mit den Sicherheitsexperten der Hersteller diskutieren und hakte bei Volkswagen, Daimler und BMW nach. Keiner der drei Hersteller wollte sich einem Gespräch stellen (siehe Kommentar). Daimler und BMW reagierten mit vorgefertigten, sehr allgemein gehaltenen schriftlichen Statements. Die Stuttgarter verwiesen auf „bekannte Sicherheitsmechanismen gemäß den Empfehlungen des BSI“ und versicherten: „Datensicherheit, Datenschutz und Diebstahlschutz sind wichtige Bausteine unserer Forschungs- und Entwicklungsaktivitäten“, das Unternehmen halte sich stets auf dem aktuellen Stand der Technik. BMW verlautbarte ähnliche Allgemeinplätze: „Entwicklungsbegleitend finden regelmäßig Penetrationstests und Security-Audits von internen Spezialisten und externen Partnern statt.“ Die VW-Pressestelle ließ drei Anfragen für einen Gesprächspartner auf Fachseite unbeantwortet.

Autoren: Daniela Hoffmann, Ulrich Hottelet