DER ZWEIFEL FÄHRT MIT

Schöne neue, mobile Welt: Während der autonom fahrende Wagen wie von Zauberhand gesteuert über die Straßen gleitet, lehnt sich der Fahrer entspannt zurück, erledigt Korrespondenzen mit dem Tablet, schaut sich einen Film an oder macht einfach ein Nickerchen. Die überwiegende Mehrheit der Deutschen, US-Amerikaner und Chinesen vertraut dem Autopiloten – gleichwohl gibt es Bedenken in Sachen Cybersecurity.

Autor: Norman Hübner **Redaktion: Diana Künstler**

➤ Die Cybersecurity-Bedenken hinsichtlich des autonomen Fahrens gibt es zu Recht, wie das Experiment eines Forscherteams demonstriert. Die Wissenschaftler drangen in die Elektronik eines Jeeps ein und konnten das Auto per Fernzugriff beschleunigen, abbremsen sowie Sicherheits- und Schutzsysteme wie Airbags, ABS und Türverriegelung lahmlegen. Dafür nutzten sie eine Schwachstelle der Software-Update-Funktion und kaperten das SUV per Mobilfunk.

Wie repräsentative Studien von TÜV Rheinland belegen, ist gerade beim autonomen Fahren die Angst vor Cyperattacken ausgeprägt. Zwar können sich drei von vier Autofahrern in Deutschland vorstellen, sich autonom chauffieren zu lassen, doch bei rund 60 Prozent dominiert die Furcht vor dem Verlust der Kontrolle des Fahrzeugs durch Hacker. Das „Entscheidungsverhalten autonomer Fahrzeuge bei der Auswahl von Alternativen im Falle unvermeidbarer Unfälle“ spielt für die Autofahrer eine ebenso entscheidende Rolle wie die „Beherrschbarkeit komplexer Verkehrssituationen“ und die Absicherung der Daten. Für die überwiegende Mehrheit der Befragten ist es daher wichtig, dass unabhängige Institutionen autonome Fahrzeuge testen sowie den Datenschutz und die Datensicherheit überwachen. Dabei stehen Fahrzeugtests zur Zuverlässigkeit der Automatisierung vor Auslieferung autonomer Autos an erster Stelle (mehr als 91 Prozent).

Ähnliches gilt für die wichtigen Märkte USA und China. Damit sie künftig autonomen Fahrzeugen vertrauen können, wünschen sich Autofahrer auch dort die Gewährleistung des Datenschutzes, die Sicherung des Fahrzeugs vor Cyberangriffen und die zu jedem Zeitpunkt freie Entscheidung, selbständig oder autonom fahren zu können. Die meisten Kunden finden es gut, dass die Systeme künftiger Autos regelmäßig automatisch aktualisiert werden, um die Sicherheit im Straßenverkehr und gegen Fremdangriffe von außen zu gewährleisten. In China befürworten solche sogenannten Over-the-Air-Updates 80 Prozent, in den USA 68 Prozent und in Deutschland 64 Prozent. Darüber hinaus ist den Verbrauchern der Schutz vor Cyberattacken in allen drei Ländern so wichtig, dass die Mehrheit die Automarke, in einem Fall von bekannt gewordenen Hackerangriffen, wechseln würde.

Grundsätzlich kommt autonomes Fahren bei den Befragten gut an. Gleichwohl nehmen sie Probleme wahr, die eine Akzeptanz beeinträchtigen können und wesentliche Hindernisse für die Verbreitung autonomer Fahrzeuge darstellen. An erster Stelle der wichtigsten Rahmenbe-

CYBERSICHERHEIT IST DER NEUE RISIKOFAKTOR FÜR DEN AUTOMOBILSEKTOR

➤ Synopsys und SAE International haben die Studie „Securing the Modern Vehicle: A Study of Automotive Industry Cybersecurity Practices“ veröffentlicht. Der Report basiert auf einer Umfrage des Ponemon-Instituts unter IT-Sicherheitspraktikern und Ingenieuren aus der Automobil- sowie Zuliefererindustrie und hebt Herausforderungen und Defizite in der Cybersicherheit von Automobilkomponenten hervor. Im Folgenden die Schlüsselergebnisse der Studie:

- **Mangel an Cybersicherheitskenntnissen und -ressourcen:** Über die Hälfte der Befragten gaben an, dass ihr Unternehmen weder genügend Budget noch Mitarbeiter für Cybersicherheit zur Verfügung stelle. 62 Prozent antworteten, dass dringend benötigte Cybersicherheitsfähigkeiten in der Produktentwicklung fehlten.
- **Proaktive Cybersicherheitstests stehen hinten an:** Weniger als die Hälfte aller Organisationen testen ihre Produkte auf Sicherheitsschwachstellen. Gleichzeitig glauben 71 Prozent, dass der Druck, Produktionsfristen einzuhalten, zu Defiziten in der Produktsicherheit führt.
- **Entwickler brauchen Cybersicherheitstraining:** Nur 33 Prozent der Befragten berichteten, dass Entwickler in ihrem Unternehmen sicheres Programmieren lernen. Zusätzlich nannten 60 Prozent mangelndes Verständnis von oder fehlendes Training zu sicheren Programmierpraktiken als primäre Faktoren, die Schwachstellen nach sich ziehen.
- **Cybersicherheitsrisiken lauern in der gesamten Lieferkette:** 73 Prozent der Befragten zeigten sich besorgt über die Cybersicherheit der Automobiltechnologien, die von Dritten zugeliefert werden. Nur 44 Prozent gaben an, dass ihr Unternehmen den eigenen Zulieferern feste Anforderungen in puncto Cybersicherheit auferlegt.

Quelle: „Securing the Modern Vehicle: A Study of Automotive Industry Cybersecurity Practices" (2018), Ponemon Institute im Auftrag von SAE International und Synopsys

dingungen von Politik und Industrie steht bei den Deutschen die Möglichkeit, selbst fahren zu können, gefolgt von der Klärung der Rechtslage und der Gewährleistung des Datenschutzes. Bei den Amerikanern hat die Möglichkeit, selbst das Steuer übernehmen zu können, ebenfalls eine hohe Priorität. Auf Platz zwei rangiert mit geringem Abstand der Nachweis der funktionalen Sicherheit durch Tests. Auf Platz drei folgt die Sicherung des Autos vor Fremdzugriff. Für die Chinesen ist die Sicherung der persönlichen Daten besonders wichtig, noch vor Gewährleistung des Datenschutzes und Sicherung des Fahrzeugs vor Fremdzugriff.

Die Cloud als Einfallstor

„Interessante Angriffsziele für Cyberpiraten sind beispielsweise aus dem Internet erreichbare Clouddienste, die unter anderem direkt mit Fahrzeugen kommunizieren. Theoretisch kann jedoch jede extern verfügbare Kommunikationsschnittstelle einen Einstiegspunkt für einen Angreifer darstellen. Dies können das bordeigene WLAN, Telematikdienste sowie Infotainment-, Navigations- und Assistenzsysteme sein", sagt Benedikt Westermann, Lead Security Analyst von TÜV Rheinland.

Die Bedeutung der Cybersecurity hat in den vergangenen Jahren deutlich zugenommen. Außerdem belegen die Auswirkungen einiger prominenter Angriffe, wie wichtig das Thema für die heutige Gesellschaft und Wirtschaft geworden ist. Das zeigen auch die Cybersecurity-Trends 2018 von TÜV Rheinland. Die Attacken machen zugleich die Verwundbarkeit der persönlichen Daten deutlich. Bereits im April 2017 tauchten über die bisher anonyme Gruppe „Shadow Brokers" eine Reihe von Hacking-Tools auf, die im Verdacht stehen, der US-amerikanischen National Security Agency zu gehören. Im Juli 2017 stahlen Angreifer die Daten von 145 Millionen Menschen des Finanzdienstleisters Equifax. Das Windows-Schadprogramm WannaCry und der Erpressungstrojaner NotPetya folgten und verbreiteten sich in über 150 Ländern. Das führte zu Lösegeldzahlungen von mehr als zwei Milliarden US-Dollar. Das Kurier- und Logistikunternehmen FedEx schrieb allein dem NotPetya-Angriff einen Verlust von 300 Millionen US-Dollar zu. Bei einigen namhaften Automobilherstellern führte dies sogar zum Produktionsstopps. Diese beiden berüchtigten Ransomware-Angriffe nutzten den von Shadow Brokers durchgesickerte Schwachpunkt aus. Und die potenziellen Schlupflöcher werden mit jeder Schnittstelle zahlreicher.

Es scheint inzwischen einfacher denn je, Erpresser- und Schadstoffprogramme auf dem Schwarzmarkt oder im Darknet zu kaufen und damit auch Zugang zu sensiblen Daten zu erhalten. Während Unternehmen ihre Digitale Transformation fortsetzen und Anwender „intelligente" Geräte in ihr tägliches Leben integrieren, wächst die Cyberkriminalität.

Bedrohung wächst

Mit fortschreitender Digitalisierung werden auch Fahrzeuge immer stärker vernetzt. Damit steigt gleichzeitig die Angriffsfläche. Von Bedienfeldern über Wartungs- und Reparatur-Programme (MRO = Maintenance, Repair and Operations) mit entsprechender Service-Management-Software bis hin zum klassischen GPS enthalten Autos eine erhebliche Anzahl zusätzlicher Funktionen. Wie andere vernetzte Produkte ist langfristig davon auszugehen, dass auch das vernetzte Fahrzeug zum Ziel von Cyberangriffen wird. Die Bedrohungen reichen von der einfachen unbefugten Datenerfassung bis hin zu schwereren Vergehen wie Fahrzeug- oder Eigentumsdiebstahl und Erpressung. Die Zustimmung für autonomes Fahren hängt daher maßgeblich von der IT-Sicherheit der Systeme und Technik ab.

Norman Hübner, Communication Expert, Digital Transformation & Cybersecurity, TÜV Rheinland Service

GANZHEITLICHE PRÜFUNGEN

➤ Die Entwicklungen der jüngsten Vergangenheit und die absehbare Entwicklung des Autos machen einen holistischen Sicherheitsansatz notwendig. TÜV Rheinland bietet daher als unabhängiger Prüfdienstleister beispielsweise in seiner Historie von Fahrzeugchecks ganzheitliche Prüfungen im Automobilsektor an. Gerade beim autonomen Fahren ist ein entsprechendes System gefordert. Das gilt dreifach: erstens für die klassische Homologation (die Straßenzulassung neuer Fahrzeugtypen), zweitens für die periodische Hauptuntersuchung sowie drittens für die Themen Datenschutz und Cybersecurity. Denn wer vernetzt oder autonom fährt, dessen Bewegungen werden erfasst. Zugleich eröffnen sich Möglichkeiten für Hackerattacken. Mit dem spezialisierten Geschäftsbereich für Digital Transformation und Cybersecurity will TÜV Rheinland darüber hinaus Unternehmen sowie Behörden und öffentliche Einrichtungen dabei unterstützen, innovative Technologien sicher zu nutzen.