CEO-Fraud auf dem Vormarsch >
< „Die Augen und der Blick sind die halbe Miete“

Das vernetzte Auto

Wer hat Zugriff auf die Daten aus den Fahrerassistenzsystemen?

Automatisierte und vernetzte Fahrzeuge sollen die Sicherheit erhöhen und das Fahrerlebnis verbessern

Nach einem schweren Unfall ist es für Verletzte lebenswichtig, dass ihnen so schnell wie möglich geholfen wird. Ab April 2018 müssen deshalb alle Neuwagen mit einem automatischen Notrufsystem („eCall“) ausgestattet sein. Damit setzt das Auto unmittelbar nach dem Unfall selbstständig einen Notruf ab – mit den exakten Standortdaten. Datenschützer kritisieren Einfallstore für Hacker und stellen Automobilhersteller, Versicherungen und IT-Unternehmen vor große Herausforderungen.

Chance und Risiko zugleich

Mit „eCall“ (emergency call) ausgestattete Fahrzeuge setzen den Notruf mittels sogenannter „Crash-Sensoren“ in Echtzeit an die nächstgelegene Notrufzentrale ab. Diese ist europaweit unter einer einheitlichen Nummer erreichbar. Die Notrufzentrale erhält über GPS eine genaue Standortmeldung des Fahrzeuges und hat über Mikrofon und Lautsprecher die Möglichkeit, mit den Insassen zu sprechen, um weitere Informationen über den Unfall zu erhalten. Außerdem kann sie auch weitere notwendige Informationen über die Rettungskarte abrufen und an die Retter (Feuerwehr, Polizei) übermitteln.
Der „eCall“ ist ein Beispiel dafür, dass die Mobilität der Zukunft vom vernetzten Auto geprägt wird. Auch Notbremsassistenten mit Personenerkennung und autonomer Notbremsung, die in Lkws bereits zur Serienausstattung gehören, könnten die Zahl der schweren Pkw-Unfälle schon bald deutlich reduzieren. Die fortschreitende Digitalisierung in der Automobilbranche soll aber nicht nur Menschenleben retten, sondern auch Stau- und Fahrzeiten verkürzen, die Umwelt schonen und das Autofahren insgesamt

komfortabler machen. So ermöglicht etwa BMW seinen Kunden mit dem Infotainment-Service „Connected Drive“ während der Autofahrt Hotels zu buchen, Konzertkarten zu bestellen oder Nachrichten abzurufen. Volkswagen bietet ebenfalls Infotainment-Applikationen an.
Sicherheitsexperten kritisieren vor allem den Umfang gespeicherter Fahrzeugdaten. Denn intelligente Autos produzieren enorme Mengen an sensiblen Daten zum Fahrverhalten, analysieren und übertragen sie – in erster Linie an die Autohäuser. Pkws, die über intelligente Systeme wie „Connected Drive“ vernetzt sind, können etwa auch der Autowerkstatt melden, wann welche Fahrzeuge zur Inspektion kommen. Auch weitere Schnittstellen wie Satelliten oder Ersatzteillieferanten können unter Umständen auf die Daten zugreifen. Insgesamt fahren bis zu 100 „Minicomputer“ in vernetzen Autos mit, die mit ihrer Umgebung interagieren. So entstehen zahlreiche Angriffspunkte sowohl für Freizeithacker als auch für professionelle Kriminelle. Gelingt es ihnen, vernetzte Autos zu knacken, haben sie nicht nur Zugriff auf Motorsteuerung und Bremsen. Über das Infotainment-System können sie auf das Smartphone des Fahrers zugreifen, Downloads starten, Schadprogramme aufspielen oder Kreditkartendaten stehlen.

Zugangswege für Hacker

1. Pkw-externe Angriffspunkte:

- Autohersteller: Die Konzerne betreiben große Rechenzentren, die die drahtlos übermittelten Informationen aus den Pkw verwalten und zum Teil an Partnerunternehmen übermitteln.
- Autowerkstätten: Sie spielen Software auf Pkw auf und ziehen über das Diagnosewerkzeug Daten ab. Per Mail oder Datensticks könnten die Betriebe mit Schadsoftware infiziert werden.
- Ersatzteillieferanten: Hacker können kriminelle Programm-Codes in das Betriebssystem elektronisch gesteuerter Bauteile einschleusen. Das gilt besonders für Ersatzteile, die bereits länger auf dem Markt sind.
- Satelliten: Die Autobauer verbinden sich mit ihrer Pkw-Flotte, fragen Standort und Fahrzeugdaten ab. So verbindet sich das Notrufsystem „eCall“ etwa per Satellit mit allen neuen Fahrzeugen.

2. Pkw-interne Angriffspunkte:

- Infotainment-Systeme: Hier laufen sämtliche Daten aus dem Internet ein – etwa, wenn die Fahrzeuginsassen online Musik hören, Nachrichten abfragen oder eine Reservierung vornehmen.
- Bremssysteme: Vernetzte Autos informieren sich gegenseitig über Bremsmanöver, um Unfälle zu vermeiden – auch hier können Hacker ansetzen.
- Antrieb: Einigen Kriminellen gelang es bereits, von außen die Kontrolle über die Beschleunigung zu übernehmen.

Herausforderungen an die Autoindustrie

Der Datenschutz spielt im vernetzten Auto eine große Rolle

Zwar beteuern die meisten Autohersteller, dass sie die Sicherheitslücken in Bezug auf Cyber-Angriffe bereits geschlossen hätten. In der Realität weisen aber die meisten bislang entwickelten Assistenzsysteme und Smartphone-Apps zum Teil noch gravierende Sicherheitsmängel bei der Programmierung auf. Die Herausforderung für die Autoindustrie der Zukunft besteht darin, gesetzliche Mindeststandards einzurichten – etwa regelmäßige Updates für alle Elektronikteile. Bisher tauschen Autohersteller bei einem Modellwechsel nur einen Teil der Fahrzeugelektronik aus. Geräte, die sich nicht unmittelbar auf das Fahrerlebnis oder die optische Erscheinung des Pkw auswirken, werden auch dann weiter verbaut, wenn ihre Betriebssoftware veraltet ist. Die digitale Gefahrenabwehr sollte bei den Herstellern oberste Priorität haben. Ein namhafter

Hersteller engagiert bereits regelmäßig professionelle Hacker, die gezielt die neuen Systeme und Produkte angreifen, um potenzielle Schwachstellen aufzudecken.

Wem gehören die Daten?

Ein weiterer Fallstrick sind die Rechte an den Daten. Nach den Vorgaben des Bundesdatenschutzgesetzes hat der Fahrer bzw. Halter des Fahrzeuges ein Selbstbestimmungsrecht an den im Auto erzeugten personenbezogenen Daten. Die Fahrzeughersteller haben sich in der Vergangenheit teilweise auf den Standpunkt gestellt, dass es sich bei den im Fahrzeug gespeicherten Daten lediglich um fahrzeug- und nicht um fahrerbezogene Daten handle, sodass dem Fahrer auch kein Recht an den Daten zustehe. Im Fall von „eCall“ darf das System die Positionsdaten des Unfallfahrzeugs nur im Notfall senden. Der Autofahrer muss bei der ersten Inbetriebnahme ausdrücklich zustimmen, dass er mit der Datenübermittlung einverstanden ist. Übermittelte Daten dürfen nur für Rettungszwecke erhoben und weder an Dritte weitergegeben noch für andere Zwecke genutzt werden. Verschiedene Stimmen wie der ADAC oder die Verbraucherzentrale Bundesverband fordern darüber hinaus, dass die eCall-Funktion ausschaltbar sein soll und Autofahrer selbst über die Datenübermittlung entscheiden können. Autohersteller sollen zum Einbau einer „offenen Schnittstelle“ für den Datentransfer verpflichtet werden. Damit könnten Autofahrer frei entscheiden, an wen sie ihre Fahrzeugdaten übermitteln.
KL (21.07.2017)

Folgende Artikel könnten Sie auch interessieren:

- Was passiert bei der MPU?
- Video: Mehr Sicherheit durch Fahrerassistenzsysteme
- Video: Fahrerassistenzsysteme im Einsatz
- Vorsicht vor Deep Fakes
- Fit fürs Elektroauto
- EU-Datenschutz und digitale Sorglosigkeit
- Der Einsatz von Section Control
- Vorratsdatenspeicherung – ja oder nein?
- Autonomes Fahren
- Automatisches Notrufsystem eCall

Alle Artikel dieser Kategorie

Weitere Infos für Gewerbetreibende

Pharming-Angriffe bedrohen Rechner von Verbrauchern

Gefährlicher als Phishing?

Das Pharming ist eine relativ neue Form der Cyberkriminalität, die...[mehr erfahren]

Die Bundespolizei ermittelt gegen Schleusernetzwerke

Migration auf dem Luftweg

Die lebensgefährliche Route über das Mittelmeer oder in Lkws sind für...[mehr erfahren]

So handeln Sie als Gewerbetreibender im Schadensfall

Den Versicherer gleich anrufen!

Wenn es in einem gewerblichen Gebäude brennt oder ein Unwetter...[mehr erfahren]

Internet-Kriminalität schädigt die Wirtschaft

Cybercrime – Angriffe auf Unternehmen

Gehackte Unternehmensnetzwerke und Diebstahl sensibler Daten von...[mehr erfahren]

Sicherheitstipps für Gewerbetreibende

Kartenzahlung im Handel

Das bargeldlose Bezahlen ist aus der modernen Geschäftslandschaft...[mehr erfahren]

Cookie Einstellungen

☐Statistiken
☐Essentiell

Wir nutzen Cookies auf unserer Website, die in unserer Datenschutzerklärung beschrieben sind. Wir verwenden anonyme Statistiken, um unsere Website zu verbessern. Bitte unterstützen Sie unsere wichtige Präventionsarbeit und akzeptieren Sie alle Cookies. Vielen Dank!

Nur essentielle Cookies akzeptierenAlle akzeptieren