Verband der TÜV e.V.

TÜV®

Autor
Richard Goebelt

Datum
15. Januar 2018

Datenschutz, IT-Security & Compliance als Basis für neue Geschäftsmodelle in der digital vernetzten Mobilität

Daten aus Fahrzeugen gewinnen in den Geschäftsmodellen der Automobilbranche immer mehr an Bedeutung. Die Nutzung dieser Daten muss aber den Beschränkungen durch Datenschutz, Sicherheit und Wettbewerbsrecht unterliegen. Das Konzept einer sicheren und neutralen Plattform innerhalb und außerhalb des Fahrzeugs, das der VdTÜV mit der Automotive Platform und dem TrustCenter vorschlägt, ermöglicht die kommerzielle Nutzung unter Berücksichtigung der berechtigten Interessen aller Beteiligten vom Fahrzeugnutzer über den Hersteller bis zu Anbieter von Drittdienstleistungen. Insbesondere bei der Weiterentwicklung der Hauptuntersuchung zu einer kontinuierlichen Überprüfung der Fahrzeuge ist eine neutrale und vollständige Bereitstellung der relevanten Daten unabdingbar.

Daten stellen ein Wirtschaftsgut dar, für deren Nutzung rechtliche und ökonomische Rahmenbedingungen geschaffen werden müssen!

Das moderne Automobil ist nicht länger nur Hardware, sondern vielmehr eine Komponente eines digital vernetzten Systems. Die Sicherheit des Automobils und die Gestaltung des Mobilitätsmarkts werden entscheidend durch die beste und aktuellste Software für die jeweiligen Fahrzeugkomponenten über den gesamten Fahrzeuglebenszyklus definiert. Durch die Vernetzung von Fahrzeugen und Fahrzeugen mit der Infrastruktur sind neue Dienstleistungen möglich, die das Potential haben, den Dienstleistungsmarkt im Bereich Automotive weitreichend zu verändern.

Erst eine umfassende sicherheitsrelevante Betrachtung und Bewertung datenbasierter Mobilitätsdienste und digitaler Funktionalitäten im Fahrzeug schaffen das notwendige Vertrauen und die Akzeptanz in der Automobilbranche zwischen Hersteller, Zulieferer und Aftermarket sowie in der Bevölkerung. Aus Sicht des Verbands der TÜV e.V. erfordert der Schutz der persönlichen Daten sowie der Schutz vor Cyberattacken besondere Security-Anforderungen für Fahrzeuge, die bereits während der Entwicklung sowohl im Auto auch als in dem damit verbundenen System betrachtet und realisiert werden müssen (Security & Privacy-by-Design).
Ziel politischen Handelns sollte es sein, Lösungen zu forcieren, die einen möglichst großen und wettbewerbsoffenen Mobilitätmarkt etablieren, in dem alle Dienstleister und Drittanbieter eine gleichwertige, angemessene und diskriminierungsfreie Ausgangslage haben. Erstens können sie so den jeweiligen Anwendern ihre digitalen Dienste im Fahrzeug sicher und datenschutzkonform anbieten. Zweitens kann sich so eine hohe Innovationskraft entfalten und Verbraucherschutz in den Bereichen Automotive und Mobility gewährleistet werden.

Datenschutz, IT-Sicherheit, Nutzerkomfort und Wettbewerbsrecht können in Einklang gebracht werden!

Hierfür sind aber aus unserer Sicht eine regulative Begleitung der Entwicklung durch rechtliche Maßnahmen des Gesetzgebers in Abstimmung mit den EU-Institutionen (gezielte Schließung von Schutzlücken bis hin zu einem „Datengesetz“) und außerrechtlichen Maßnahmen (Förderung eines einheitlichen Marktes durch Standardisierung, Förderung des Bewusstseins etc.) kurz- und mittelfristig notwendig.

Alle Konzepte der Automobilindustrie gehen von der Grundannahme aus, dass die relevanten Fahrzeugdaten zunächst an einen Server im Verfügungsbereich des Fahrzeugherstellers (Backend) gesendet und verarbeitet werden. Diese Konzepte können nur als Zwischenlösungen betrachtet werden, entfalten aber in keiner Weise die technologischen Möglichkeiten einer kooperativen, automatisierten und vernetzten Mobilität der Zukunft. Produktsicherheit und Produkthaftung, wie von den Fahrzeugherstellern angeführt, begründen weder ein ausschließliches Datenverarbeitungsrecht in Backend-Servern einzelner Hersteller, noch kann damit allein begründet werden, dass Dritte nicht direkt auf die Fahrzeugdaten zugreifen dürfen. Entscheidend bleibt, dass der Fahrer selbst die Wahl hat, wie er mit seinen Daten umgehen möchte. Darum müssen die Kunden Cloud-basierter Dienstleistungen in der Mobilität souverän entscheiden können, welche Daten sie preisgeben und was mit ihren Daten passiert. Ihnen muss es möglich sein, die Datenübermittlung zu erkennen, zu kontrollieren und gegebenenfalls auch zu stoppen.

TrustCenter in Kombination mit Automotive Platform sind das Fahrzeug der Zukunft

Mit dem Konzept des TrustCenters möchte der Verband der TÜV e.V. einen eigenen Diskussionsbeitrag leisten und die bestehenden Ansätze zur Datennutzung um die Idee einer sicheren, neutralen und datenschutzkonformen Cloudbasierten Lösung ergänzen. Der Fahrzeughalter und -fahrer soll von der Verwendung der eigenen Daten durch Cloudbasierte Dienste profitieren und insbesondere – in Abgrenzung zu anderen Konzepten – auch die vollständige Transparenz und Datensouveränität erhalten, die das TrustCenter in Kombination mit einer IT-Sicherheitsarchitektur in einem digital vernetzten Fahrzeug (Automotive Platform) realisiert. Er kann entscheiden, welchem Dienstleister er wann und unter welchen Konditionen die Daten freigibt. Das TrustCenter schafft entsprechend der Compliance-by-Design-Grundsätze und des Grundsatzes der Datenneutralität technische Vorkehrungen, die Wettbewerbsbeschränkungen vorbeugen. Automobilhersteller und andere Dienstleister können ihre Dienstleistungsangebote an den Eigentümer bzw. Halter des Fahrzeugs unterbreiten, ohne die Daten und Datenströme des Wettbewerbs permanent auslesen zu können. Dabei wird vorausgesetzt, dass ihre Server die Kriterien des TrustCenter erfüllen. Denn dieser trennt die Aufgaben der Instanz, die die Zugangsberechtigung erteilt, von denen der Instanz, die datenbasierte Dienstleistungen anbieten möchte.

Für die IT-Sicherheit und die Berücksichtigung der gesetzlichen Datenschutzanforderungen (Security & Privacy by Design) empfiehlt der VdTÜV zudem die Verwendung einer neuen, hochsicheren Automotive Platform, die mit einem entsprechenden Interface im Fahrzeug die Kommunikation innerhalb des Systems und nach außen absichert. Diese Komponente ist dringend notwendig, um u. a. Car2X-Funktionalitäten zukünftig sicher anbieten zu können. Entsprechend des Automotive Platform Konzepts werden die verschiedenen IT-Systeme im Auto logisch voneinander getrennt. Entertainment und Komfortsysteme sind nur über die Sicherheitsarchitektur mit sicherheits- und emissionsrelevanten Systemen verbunden. Der Zugang über einen On-Board-Diagnose-Stecker (OBD) oder eine Telematikschnittstelle (TCU) auf die elektronischen Systeme des Fahrzeugs bleibt somit auch in Zukunft mit einer hochsicheren IT-Sicherheitsarchitektur im Fahrzeug möglich.

Die Konzepte des TrustCenter und der Automotive Platform ermöglichen in ihrer Kombination einen direkten, sicheren und datenschutzkonformen Zugriff auf das Fahrzeug. Im Fahrzeug erzeugte Daten werden über die Automotive Platform sicher und transparent an ein TrustCenter zur Bereitstellung weiterer Funktionalitäten durch Partner und Dienstleister übermittelt.

Relevanz für die Weiterentwicklung der HU

Technisch sind die Überwachungsorganisationen der TÜV mit dem HU-Adapter heute in der Lage, das bestimmungsgemäße Vorhandensein und den Funktionsstatus von sicherheitsrelevanten elektronischen Systemen zu prüfen sowie unerlaubte Manipulationen und illegales Tuning beim Motormanagement und der Abgasreinigung zu detektieren. Der HU-Adapter erfüllt damit seit 2015 die Forderungen der EU-Kommission. Nach wie vor mangelt es aber an der Kooperationsbereitschaft einer Reihe von Fahrzeugherstellern zur Bereitstellung von entsprechenden Diagnosedaten und Softwareversionen, obwohl die rechtliche Grundlage gemäß VO (EG) 715/2007 und VO (EG) 595/2009 dies bereits heute fordert. Somit sind wir heute oftmals gezwungen, über aufwendige Reengineering-Verfahren die relevanten Daten selbst zu ermitteln. Diese Möglichkeit der originären Kontrolle durch unabhängige Dritte wird zukünftig ebenfalls in Frage gestellt. Denn das Kernelement des vom VDA vorgestellten Konzepts besteht darin, die OBD-Schnittstelle im Fahrzeug zu schließen – jedenfalls Schritt für Schritt und insbesondere während des Fahrbetriebs.

Ein HU-Prüfverfahren nach heutigem Vorbild bei automatisierten Fahrfunktionen spätestens ab Stufe 3 (hochautomatisiertes Fahren) erscheint zudem derzeit nicht mehr angemessen, valide Prüfaussagen zu treffen. Ab Stufe 3 steigen die Systemkomplexität und die Situationskombination, in denen das System überwacht werden muss, exponentiell an. Insoweit ist eine Ergänzung der Hauptuntersuchung durch eine persistente automatisierte OBD-Systemüberwachung durch unabhängige, kompetente Stellen erforderlich.
Dadurch können die elektronischen Systeme kontinuierlich überwacht und müssen nicht im Rahmen der periodischen Hauptuntersuchung überprüft werden. Die HU dieser Systeme kann

somit beispielsweise nach kritischen Softwareupdates oder nach individuellen Emissionsvorgaben in Echtzeit erfolgen. Voraussetzung hierfür ist ein direkter Zugriff auf die sicherheits- und emissionsrelevanten Komponenten und deren digitalen Identifikationsparameter über den gesamten Lebenszyklus des Fahrzeugs. Die periodische Untersuchung würde sich dann stärker auf die Hardware und mechanische Komponenten fokussieren.

Die funktionale Sicherheit, die Security sowie die Integrität der Software einzelner Fahrzeugkomponenten des Fahrzeugs können über einen hochsicheren Datenverkehr zwischen Fahrzeug, Trustcenter und/oder unabhängiger Überwachungsinstitution im gesamten Lebenszyklus überwacht werden. Die Unabhängigkeit der Hauptuntersuchung von Herstellervorgaben, ihre Aussagekraft hinsichtlich der elektronischen und digitalen Systeme und die Gleichmäßigkeit werden damit gesteigert.

Das Ziel muss sein, rechtlich und regulatorisch mit der technischen Entwicklung Schritt zu halten, um das Sicherheitspotenzial von Digitalisierung, Vernetzung und Automatisierung des Verkehrs im Interesse der Bevölkerung wie der Wirtschaft bestmöglich nutzen zu können. Die periodisch technische Überwachung wird für die Straßenverkehrssicherheit in Zukunft unter den entsprechenden Bedingungen weiterhin ihren maßgeblichen Beitrag leisten und mit der Digitalisierung Schritt halten.