PI 03-11/2022-PG
Donnerstag, 24. November 2022

Datenzugang zu vernetzten Fahrzeugen

- **Restriktiver Datenzugang widerspricht gesetzlichen Regelungen**
- **Cybersecurity – berechtigte Sicherheitsbedenken oder Werkzeug für Datenmonopole?**
- **Verbändeallianz kämpft für liberalisierten Datenzugang im IAM**
- **Fairer Datenzugang – künftig nur noch per Gerichtsprozess?**

Harald Hahn, Leiter des Fachbereichs Diagnose- und Abgasmessgeräte im Bundeverband der Hersteller und Importeure von Automobil-Serviceausrüstungen e.V., gewährte anlässlich der ASA-Jahrespressekonferenz 2022 einen Blick hinter die Kulissen der Lobbyarbeit im Freien Reparaturmarkt. Dort kämpft der ASA-Bundesverband zusammen mit anderen europäischen Verbänden für einen fairen und diskriminierungsfreien Zugang zu technischen Daten vernetzter Fahrzeuge. Der Kampf um Datenzugänge, stellvertretend für alle an Reparatur-, Service- und Verkaufsprozessen beteiligten Akteure bis hin zum Endverbraucher, ist an sich nicht neu. Doch mit der fortschreitenden Vernetzung und Digitalisierung der Fahrzeugdateninfrastrukturen hat dieser Kampf eine neue Qualität bekommen. „Wir kämpfen zunehmend auch gegen die Zeit, denn die Automobilhersteller schaffen mit ihren abgeschotteten technischen Lösungen seit Jahren Fakten. Die europäische und nationale Politik hinkt diesen Entwicklungen in ihrem Bemühen um marktgerechte Regulierung teilweise um Jahre hinterher“, sagt Hahn.

Gegen geltendes Recht
Und selbst bestehende gesetzliche Regelungen garantieren offensichtlich nicht, dass klare Zugangsregeln im Markt auch umgesetzt werden. Beispiel Typzulassungsrichtlinie EU 2018/858. „In der Richtlinie ist der Datenzugang über den OBD-Port der Fahrzeuge eindeutig geregelt. Dennoch haben Automobilhersteller diese klaren Regeln beispielsweise mit dem Hinweis auf Cybersecurity umgangen oder außer Kraft gesetzt und damit große Teile des Reparaturmarktes zunächst ausgeschlossen“, sagt Hahn.

Eine weitere Herausforderung: In der Richtlinie 2018/858 ist nur der Datenzugang über OBD-Port geregelt. „Datenzugänge „over the air“ die bei Fahrzeugen jüngster Bauart heute fast schon Standard sind, hat man in dem Regelwerk überhaupt nicht behandelt“, so Hahn.

„Bei Cybersecurity berufen sich die Automobilhersteller auf die UN-ECE-Regelung 155. Die ist formal noch nicht in den europäischen Richtlinien verankert, hat also für den europäischen Markt de facto keine Gültigkeit“, verdeutlicht Harald Hahn. Dennoch hätte die Automobilindustrie die Datenzugänge zu ihren Fahrzeugen im Vorgriff und mit Verweis auf die ECE-Regelung abgeschottet und kontrollierte Zugriffe für den IAM nur über so genannte Zertifikate ermöglicht.

Zertifikate-Wildwuchs überfordert IAM

Dabei stehen Diagnosegerätehersteller und Werkstätten vor der Herausforderung, dass jeder Hersteller seine eigene Zertifikate-Regelung pflegt. „Es gibt keine einheitlichen Lösungen, für die beispielsweise die Diagnosegerätehersteller den Entwicklungsaufwand nur einmal betreiben müssten“, verdeutlicht Hahn. Jeder Automobilhersteller verfolgt seine eigene „Philosophie“ von Cybersecurity, wie die Beispiele von Mercedes-Benz und Volkswagen verdeutlichten.

„Während bei Mercedes-Benz über die OBD-Schnittstelle ohne Zertifikate-Anmeldung ausschließlich die für Haupt- und Abgasuntersuchung erforderlichen Daten auslesbar sind, lassen sich bei Volkswagen ohne Zertifikat Fehlercodes lesen und löschen, Messwerte lesen oder die Serviceanzeige zurücksetzen“, erklärt Hahn. Seien Volkswagen deswegen in Sachen Cybersicherheit weniger sicher als Fahrzeuge von Mercedes-Benz?

Überflüssiger Zusatzaufwand

Die unterschiedlichen Cybersecurity-Philosophien der Automobilhersteller haben im Markt zu einem wahren Wildwuchs an Zertifizierungsverfahren für den Datenzugang geführt. „Dieser Wildwuchs verursacht bei Geräteherstellern und Werkstätten aktuell enorme personelle und finanzielle Zusatzaufwände“, sagt Harald Hahn.

Dabei sind die Zertifikate-Verfahren rein technisch gesehen völlig überflüssig: „Eine Diagnosesitzung läuft gemäß ISO-Standards nach vordefinierten Befehlen ab – alles andere außerhalb dieser Befehle ist nicht möglich bzw. kann im Fahrzeug unterbunden werden“, stellt Harald Hahn klar.

Für den Fachbereichsleiter Diagnose ist klar, dass es bei den Cybersecurity-Zertifizierungsverfahren dringend zu einer Vereinheitlichung kommen muss. „Es kann im Zeitalter der Digitalisierung nicht sein, dass jeder Tool-Hersteller für jeden Automobilhersteller separat ein eigenes Zertifizie-

rungsverfahren in seine Tools integrieren muss. Und es ist auch nicht vertretbar, dass sich jeder Mechaniker einer Werkstatt separat beim Automobilhersteller autorisieren muss und sich dabei die Autorisierungsverfahren von Hersteller zu Hersteller auch noch unterscheiden“, sagt Hahn.

Einen Vorschlag für eine einheitliche und sichere Lösung gibt es bereits mit dem SERMI-Verfahren (bisher nur für diebstahlrelevante Dinge etabliert). Dieses könnte entsprechend erweitert oder angepasst werden (Vorschlag ZDK: SERMA).

Das Ziel heißt Secure Open Telematics Platform (S-OTP)
„Wir engagieren uns als ASA-Bundesverband in der ZDK-Arbeitsgruppe Telematics zusammen mit anderen Organisationen für einen fairen, wettbewerbsfähigen Zugang zum Fahrzeug“, sagt Harald Hahn. Mitstreiter in der Arbeitsgruppe sind neben den Werkstätten und Autohäusern im ZDK auch die Versicherungswirtschaft, die Teile- und Reifenindustrie, Autoverleiher und Verbraucherverbände. „Das gemeinsame Engagement zielt dabei nicht nur auf den fairen Zugang zu Daten; auch der Zugang zu weiteren Funktionen im Fahrzeug, beispielsweise der Implementierung von Apps, gilt unser Engagement“, stellte Harald Hahn klar.
Kernforderung der Arbeitsgruppe ist die Schaffung einer so genannten Secure-Open Telematics Platform (S-OTP), die unabhängig von den Automobilherstellern alle erforderlichen Daten vollständig und in Echtzeit für den IAM bereitstellt. Aktuelle Implementierungen von Polestar 2 (Android Automotive) und Volkswagen (Continental ICAS) zeigen, dass dies bereits auf Basis der bestehenden Infrastruktur möglich ist.

Nicht ohne einen Anwalt?
Auf dem Weg zu einem fairen, diskriminierungsfreien Datenzugang für Unternehmen des Independent Aftermarket scheinen aktuell juristische Auseinandersetzungen das wirksamste Mittel zu sein, um zeitnah eine Lösung herbeizuführen.
„Beim Europäischen Gerichtshof EUGH sind aktuell drei Verfahren gegen Fahrzeughersteller anhängig. In allen drei Verfahren steht die Auslegung der Typzulassungsrichtlinie EU 2018/858 im Mittelpunkt“, erklärt Harald Hahn. Beklagte sind die Hersteller PSA, Scania und FCA. Kläger sind die Independent Automotive Data Publisher (ADPA), der Gesamtverband Autoteilehandel (GVA) sowie gemeinsam ATU und Carglass.

„Als ASA-Bundesverband unterstützen wir diese Aktivitäten im Rahmen unserer Europäischen Partnerschaften (EGEA/AFCAR). Für die gesamte Branche und den IAM insgesamt ist es von existenzieller Bedeutung, dass hier über die juristische Klärung eindeutige Antworten gegeben werden“, sagt Harald Hahn abschließend.

Weitere Informationen:

Geschäftsstelle
ASA-Bundesverband
Amselweg 2a
85591 Vaterstetten

Telefon: +49 8106 99960-27
Fax: +49 8106 99960-34
E-Mail: geschaeftsstelle@asa-verband.de
Internet: www.asa-verband.de