Foto: Bosch

Der schreibende Zugriff bei der Fahrzeugdiagnose wird künftig nur noch mit SGW-Lösungen möglich sein.

Auf sicheren Wegen

Security Gateway | Das Thema Datensicherheit steht bei den Fahrzeugherstellern ganz oben auf der Agenda. Die Lösungen der Automobilindustrie bedeuten für Kfz-Werkstätten aber zusätzliche Kosten und erheblichen Mehraufwand.

Kurzfassung

Niemand zweifelt, dass auch die Software von Fahrzeugen vor Manipulation gesichert werden muss. Doch wie das geschehen soll, darüber wird heftig zwischen Fahrzeug- und Diagnosegeräteherstellern diskutiert. Welche Auswirkungen das auf die Kfz-Werkstätten haben könnte, zeigt unser Bericht.

Für Fiat Chrysler war es ein Desaster. Zwei Hackern gelang es 2015, auf wichtige Funktionen wie Bremse, Einspritzung und Türverriegelung während der Fahrt zuzugreifen und nach ihren Wünschen zu beeinflussen. Die Angreifer nutzten bei Fiat die Konnektivitäts- und Diagnoseprotokolle zur Modifikation der Software der beteiligten Steuergeräte. Doch nicht nur bei Fiat hat dieser Vorfall eine Lawine losgetreten. So sind bereits jetzt der Golf 8, die S- und E-Klasse von Mercedes und einige Modelle von Audi, Seat, Skoda, KIA und Renault/Nissan mit einer Security-Gateway-(SGW-)Lösung ausgestattet, die den Zugang zum Steuergerät sichert. Einfach gesagt, der Fahrzeug-CAN-Bus wird verriegelt. Wie das genau geschieht, ist Sache der Programmierer. Erst der Austausch von digitalen Berichtigungen (sogenannte Zertifikate, Token oder Keys bzw. Seed-und-Key-Verfahren) zwischen dem Diagnosegerät am Fahrzeug und dem IT-Backend des Herstellers öffnet den CAN-Bus und damit das Steuergerät. Problem ist, dass die Art der Umsetzung, wie Häufigkeit des Zertifikatsaustausches oder die Notwendigkeit einer Online-Dauerschaltung während der Diagnose, alleine dem Fahrzeughersteller obliegt. Für markenübergreifend arbeitende Werkstätten bedeutet dies einen enormen Aufwand bei Authentifizierung und Recherche in den OE-Portalen, da mittlerweile mit SGW bei allen Modellreihen, die neu homologiert werden, gerechnet werden muss.

Für die Arbeit der Kfz-Werkstätten heißt dies, dass ohne Zugangserlaubnis (Security-Pass) zum Steuergerät nicht schreibend zugegriffen werden kann. Somit lassen sich weder Fehlercodes löschen noch Service-Rückstellungen, noch lassen sich Updates durchführen. Hinzu kommt,

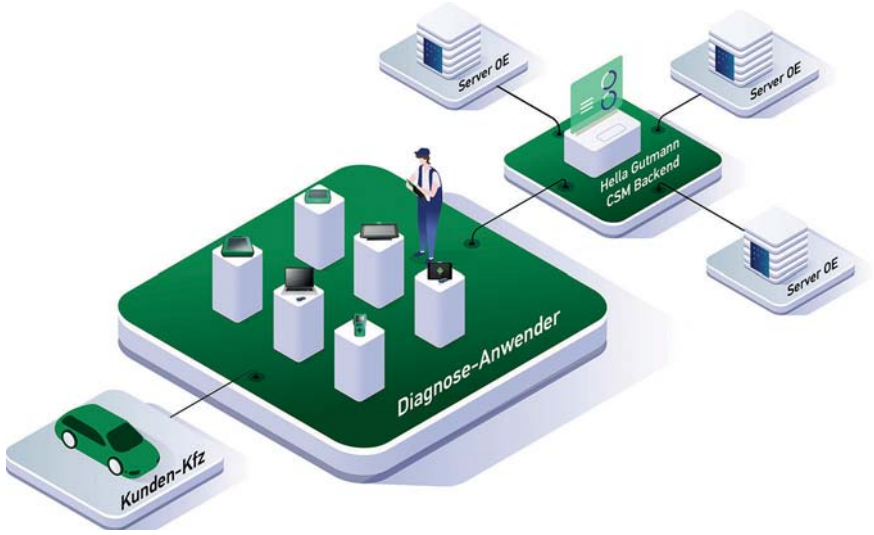

Foto: Hella Gutmann

Mit Cyber Security Management bietet Hella Gutmann einen Universalschlüssel für die Diagnose.

dass die Fahrzeughersteller unterschiedliche Bereiche der Software vor unberechtigtem Zugriff schützen. „Hier ist bisher nichts einheitlich geregelt", so Harald Hahn, Vizepräsident Bundesverband der Hersteller und Importeure von Automobil-Service Ausrüstungen (ASA). „Es hängt sehr stark von der Philosophie des Fahrzeugherstellers ab, was und welche Bereiche er im Sinne der Cybersecurity für schützenswert hält." Hier zeigt sich das ganze Dilemma, insbesondere für Diagnosegerätehersteller und Werkstätten, denn jeder Fahrzeughersteller hat offenbar seine eigene Definition, wie Angriffe auf das Fahrzeug aussehen könnten. „Doch selbst wenn hier einheitliche Lösungen vorliegen, könnten Fahrzeughersteller nicht so ohne weiteres den schreibenden Zugang zur OBD nach eigenem Gusto reglementieren", erklärt Hahn. „Zum Thema Diagnosefunktionen muss man nämlich klar herausstellen, dass diese Vorgehensweise in der aktuellen Gesetzgebung nicht vorgesehen und damit auch nicht zulässig ist. Weder in der bisherigen Verordnung EG 715/2007 noch in der aktuellen Verordnung EU 2018/858 ist davon die Rede beziehungsweise sind derartige Restriktionen vorgesehen. Im Annex X Abschnitt 2.9 (*siehe Kasten*) wird sogar eindeutig auf den freien Zugang über den OBD-Port verwiesen."

Foto: ASA

Harald Hahn, Vizepräsident des ASA-Verbandes, sucht nach kundenfreundlichen Lösungen.

Nicht gesetzeskonform

Nach Ansicht des ASA-Verbandes ist die aktuelle Zugangsrestriktion via SGW keineswegs konform zur gültigen Gesetzgebung. Der ASA-Verband arbeitet daher mit seinem europäischen Partner EGEA (European Garage Equipment Association) und anderen Verbänden intensiv an dieser Thematik. So wurden schon Zulassungsbehörden in Europa angeschrieben und um Stellungnahme gebeten, da mit SGW gesicherte Fahrzeuge hinsichtlich OBD-Zugriff nach Auffassung der Verbände nicht den aktuellen Gesetzen entsprechen.

Doch die Probleme reichen noch viel weiter. So ist eine der Kernforderungen von ASA und EGEA, eine standardisierte Lösung zur Authentifizierung der Kfz-Werkstatt beim OBD-Zugang zu erarbeiten. „Aktuell hat jeder Fahrzeughersteller sein eigenes System implementiert, was so nicht akzeptabel ist", so Hahn. „Wir fordern daher einen einheitlichen Rahmen (Standard), der für alle Fahrzeughersteller gleich ist." Nach Meinung des ASA-Verbandes muss die Authentifizierung einheitlich über unabhängige Trust Center erfolgen und nicht über den Fahrzeughersteller. Harald Hahn: „So könnte die Authentifizierung am sogenannten Sermi-Prozess angelehnt sein, der bereits für Arbeiten an diebstahlrelevanten Systemen, wie Schlüssel-Erstellen, Wegfahrsperre-Codieren, verwendet wird." Wie darüber hinaus zukünftig die Prüfung der „Vertrauenswürdigkeit" einer Werkstatt oder der Nutzerperson aussehen wird, ist ebenfalls noch offen. Auch hier sucht der ASA-Verband Lösungen.

Ähnlich ungeklärt ist die Art der Zertifikate, die man nach der Authentifizierung erhält. Sie könnten, wie der ASA-Verband annimmt, zeitlich limitiert und von bestimmten Diagnosefunktionen und Reparaturprozessen abhängig sein. Auch könnten die Zertifikate nicht nur an das Diagnosetool gebunden sein, sondern auch an die Person, die Reparaturen oder Diagnosen am Fahrzeug ausführt. Hier haben die Hersteller die Produkthaftung im Visier, um nachzuvollziehen, welche Arbeiten am Fahrzeug wann ausgeführt wurden. Der ASA-Verband sieht dies als äußerst problematisch an. Er schlägt daher vor, dass der Toolhersteller eine gewisse Anzahl Zertifikate vorhält und diese dem Nutzer verkauft, sodass das Handling über den Mehrmarkentool-Hersteller abgewickelt wird. Auch die Art der Prüfung der „Vertrauenswürdigkeit" einer Werkstatt oder der Nutzerperson ist noch offen.

Vor diesem Hintergrund versuchen die Diagnosegerätehersteller ihren Kunden praktikable Lösungen anzubieten. So hat

Das sagt die Verordnung

In der aktuellen Verordnung EU 2018/858 wird im Annex X Abschnitt 2.9 eindeutig auf den freien Zugang über den OBD-Port verwiesen:
Für die Zwecke der Fahrzeug-OBD sowie der Fahrzeugdiagnose, -reparatur und -wartung ist der direkte Fahrzeugdatenstrom über einen seriellen genormten Datenübertragungsanschluss gemäß der UN-Regelung Nr. 83 Anhang 11 Anlage 1 Nummer 6.5.1.4 und der UN-Regelung Nr. 49 Anhang 9B Nummer 4.7.3 bereitzustellen. Befindet sich das Fahrzeug in Bewegung, so darf auf die Daten nur im Lesemodus zugegriffen werden.

Hella Gutmann jetzt mit der neuen Funktion CSM (Cyber Security Management) einen Universalschlüssel für das legale Entsperren gesicherter Fahrzeuge in die Mega-Macs-Software implementiert. Statt sich in jedem OE-Portal einzeln zu registrieren und sich prüfen zu lassen, um die Diagnosefreischaltungen zu erwirken, reicht für den Mega-Macs-Anwender eine einmalige Authentifizierung bei Hella Gutmann aus. Dafür ist ein einmaliger Identifikationsnachweis per Pass oder ID-Card ausreichend. Dann hat der Mega-Macs-Anwender freie Bahn, um an Fahrzeugen mit Sicherheitssperre in gewohnter Diagnosetiefe zu arbeiten. Das Cyber Security Management steht Anwendern der Mega-Macs-Geräte 42SE, 56, 66, 77 und Mega Macs PC automatisch ab dem Update auf die Software-Version 60 zur Verfügung. Zu den ersten integrierten Marken gehören FCA und Mercedes-Benz, gefolgt von VW und Kia. Hyundai, Nissan und Renault sollen in Kürze folgen. Die Abdeckung wird schrittweise mit den gesicherten Modellen der Hersteller wachsen.

Alles in einem mit EuroDFT

Auch die ADIS-Technology GmbH aus Aachen bietet mit ihrem EuroDFT-Diagnosegerät uneingeschränkten Zugang bei der Fahrzeug-Diagnose. Zwölf Markensysteme sind auf dem EuroDFT implementiert, darunter auch solche mit SGW, wie Mercedes-Benz oder VW. Nutzer können somit Arbeiten am Fahrzeug vollständig nach Herstellervorgaben ausführen. Um möglichst wenig bürokratischen und technischen Aufwand zu haben, übernimmt ADIS-Technology für die Anwender sowohl die Registrierung bei den Fahrzeugherstellern als auch die Updates der Herstellersoftware.

Bei AVL Ditest arbeitet man ebenfalls mit Hochdruck an Lösungsansätzen. Diese könnten aber je nach Hersteller unterschiedlich ausfallen. Beispielsweise kann der Zugriff direkt über den Diagnosegeräte-Hersteller ermöglicht werden, oder er wird über den Fahrzeughersteller und dessen Infrastruktur erfolgen. Zwingend erforderliche Voraussetzung hierfür wird aber in nahezu allen Fällen ein Internetzugang sein.

Auch Bosch will sich noch nicht festlegen, wie Diagnose via SGW zukünftig aussehen wird. Die Lösungen der jeweiligen Fahrzeughersteller weisen laut Bosch aktuell noch große Unterschiede auf. Vermutlich laufe es auf eine vorherige Registrierung der Werkstatt, Bezahlung bei dem einen oder anderen Fahrzeughersteller und die Notwendigkeit einer stabilen Internetverbindung hinaus. Dazu komme ein modernes Kommunikationsmodul (VCI), das die Verbindung zwischen dem Server des Fahrzeugherstellers und dem Fahrzeug-Steuergerät sicherstellt. Hier verweist Bosch auf das KTS 560, 590, 350 und bald auch das KTS 250, welches ein internes KTS 560 nutzt (geplant für 2021).

Bei Mahle setzt man sich zurzeit ebenfalls mit der unklaren Situation auseinander. Einen herstellerübergreifenden Zugang beim SGW beziehungsweise einheitliche Zertifikate für die schreibenden Funktionen sieht man jedoch bei dem Stuttgarter Unternehmen nicht. Lediglich bei der Authentifizierung der Werkstatt gibt man sich zuversichtlich. Hier dürfte künftig eine einfache Registrierung mit den Unternehmensdaten der Werkstatt ausreichen. Probleme mit der Konnektivität könnte es jedoch bei einigen älteren Diagnosegeräten geben, da diese nicht mehr updatefähig sein werden.

Betrachtet man diese Aussagen, lässt sich feststellen, dass es keine „Regel" bei den Fahrzeugherstellern für die Umsetzung von SGW gibt. Bestimmte Marken blockieren alle Steuergeräte, andere nur ausgewählte, welche die „Sicherheit" des Fahrzeugs beeinflussen könnten. Das macht es den Diagnosegeräte-Herstellern schwer, Lösungen zu erarbeiten. Sicher dürfte sein, dass einige Autohersteller Pauschalen, andere Pay-per-Use-Gebühren erheben werden. So oder so, die Werkstätten müssen sich wohl auf höhere Kosten einstellen.

Marcel Schoch

„Kein Grund zum Verzweifeln"

Foto: ADIS

Dirk Marichal, Geschäftsführer ADIS-Technology GmbH in Aachen

„Für jeden PC-Benutzer ist es völlig normal, sich mithilfe einer Firewall und eines Virenschutzes vor unbefugten Eindringlingen zu schützen. Sollte das im eigenen Pkw nicht auch der Fall sein?

Ich lasse mich bei Autobahnfahrten gerne durch meine Assistenzsysteme unterstützen, u.a. Abstandsradar und Spurführungsassistent. Die kommenden Fahrzeuggenerationen werden noch viel mehr können, nicht auszudenken, was wäre, wenn Hacker sich Zugriff verschaffen und Steuergeräte mit einer falschen Software bespielen würden.

Wir beschäftigen uns bei der ADIS-Technology seit vielen Jahren mit der Fahrzeugkommunikation, speziell mit Buskommunikation, Fahrzeugdiagnose und Programmierung. Für mich ist es daher nachvollziehbar, dass ein Automobilhersteller mit dem Security Gateway den Zugang zum Fahrzeug schützen möchte. Dies ist nicht nur sein gutes Recht, sondern seine Pflicht.

Jede legitimierte Werkstatt muss jedoch weiterhin Zugriff auf die Fahrzeugsysteme haben. Dies ist in der aktuellen europäischen Typengenehmigungsverordnung 2018/858 festgelegt. Der Zugang muss dabei diskriminierungsfrei und bezahlbar sein.

Die Herstellersoftware bringt deshalb in der Regel von Hause aus alle technischen Voraussetzungen mit, sodass der Zugang mit Security Gateway gewährleistet ist. Um Diagnose- und Programmiersoftware nutzen zu können, müssen jedoch, je nach Hersteller, unterschiedliche Registrierungsprozesse durchlaufen werden. Diese sind zum Teil recht komplex und der zukünftige Nutzer muss seine Daten bis hin zum Führungszeugnis offenlegen.

Das Security Gateway ist zweifellos da und wird in den kommenden Jahren in immer mehr Fahrzeugen verbaut sein. Wie üblich kocht jeder Hersteller sein eigenes Süppchen und arbeitet an unterschiedlichen Verfahren. Die Werkstatt ist damit schnell überfordert und braucht einen kompetenten Partner, der berät und bei der Umsetzung hilft. Es gibt also Anlass zum Handeln, jedoch keinen Grund zu verzweifeln."

Mobiles Arbeiten
Wortwörtlich

Den Arbeitsplatz der Zukunft? Gibt's jetzt auch auf vier Rädern. Dank Innovision Cockpit* und Sprachsteuerung* ist der neue Caddy Cargo bestens vernetzt. Und wird mit seinem umklappbaren Beifahrersitz im Handumdrehen zum mobilen Büro mit praktischer Arbeitsfläche. Mehr Informationen bei Ihrem Volkswagen Nutzfahrzeuge Partner.

Der neue Caddy Cargo. Bereit für alles, was kommt

*Sonderausstattung gegen Mehrpreis. Nur in Verbindung mit einem kompatiblen Infotainmentsystem erhältlich. Abbildung zeigt Sonderausstattung gegen Mehrpreis.

vwn.de/der-neue-caddy-cargo