

Was als Auto-Update erlaubt ist

Immer mehr Autohersteller bieten für ihre Fahrzeuge Software-Updates Over-the-Air an, die Funktionen nachrüsten oder Fehler beseitigen. Doch wie ist die rechtliche Situation?



Foto: TÜV Süd

Karsten Graef ist Sachverständiger bei TÜV Süd und Experte für Software-Updates

Herr Graef, wie ist die rechtliche Grundlage für Software-Updates Over-the-Air in Autos? Dürfen Autohersteller wie Tesla Updates ohne Werkstattbesuch auf das Fahrzeug aufspielen?

K. Graef: Ja, das dürfen Autohersteller grundsätzlich, solange dieses Software-Update mit den Gesetzen und Verordnungen des einzelnen EU-Mitgliedsstaates konform geht, in dem das Fahrzeug zugelassen ist. In Deutschland wäre hier insbesondere die Straßenverkehrs-Zulassungs-Ordnung (StVZO) zu beachten, dort ist die

Betriebserlaubnis in Paragraph 19 geregelt. Eine einheitliche Lösung in allen EU-Staaten gibt es bislang nicht. Im Sinne der Verkehrssicherheit und des Umweltschutzes sollte eine europaweit gültige Lösung – sofern möglich – entwickelt werden. Derzeit sieht das EU-Recht nur Regelungen für das Inverkehrbringen vor, also Typgenehmigung und Zulassung von Fahrzeugen.

Nehmen wir an, ein Autohersteller bietet ein Update an, das die Fahreigenschaften des Autos verändert, bei-

spielsweise mehr Leistung liefert. Ist das erlaubt?

K. Graef: Es gibt Änderungen an einem Fahrzeug, die in Deutschland zum Erlöschen der Betriebserlaubnis nach Paragraph 19 Absatz 2 StVZO führen, beispielsweise eine Verschlechterung des Abgas- oder Geräuschverhaltens oder eine Änderung der Fahrzeugart. Außerdem jede Änderung, die eine Gefährdung für Verkehrsteilnehmer darstellt. Hierunter fällt entsprechend der Richtlinie zu Paragraph 19 StVZO auch eine Leistungssteigerung – wenn für diese keine Genehmigung oder auch keine Teiletztypgenehmigung vorliegt. Ein besonderes Augenmerk sollte auch darauf gelegt werden, wenn essenzielle zulassungsrechtliche Daten nach Paragraph 13 der Fahrzeug-Zulassungs-Verordnung (FZV) betroffen sind. In dem genannten Beispiel wäre damit mindestens durch den Halter unverzüglich die Zulassungsbehörde über diese Änderung zu informieren. An der Leistungssteigerung des Fahrzeugs können neben den zulassungs- und steuerrechtlichen sowie verhaltensrechtlichen Aspekten, also dem Betrieb des Fahrzeugs, auch versicherungsrechtliche hängen.

Wer überprüft Software-Updates, bevor sie aufgespielt werden?

K. Graef: Es erfolgt, Stand heute, in aller Regel die Überprüfung einer neuen Softwareversion von einer unabhängigen Institution im Rahmen der Typprüfung. Wie gesagt, das Aufspielen auf in Verkehr befindlichen Fahrzeugen hängt dann an der jeweils nationalen Verordnung eines EU-Mitgliedsstaates. Grundsätzlich stehen also die Fahrzeughersteller selbst in der Pflicht. Es gibt noch recht neue sogenannte UN-Regelungen der Wirtschaftskommission für Europa der Vereinten Nationen (UNECE), die für die Fahrzeuggenehmigung relevant werden könnten und teilweise Regelungen mitbringen, die hier Anwendung finden können. Die UNECE hat beispielsweise zwei UN-Regelungen für

die Themen Cybersecurity und Software-Updates erlassen. In den Vorschriften steht, dass Fahrzeughersteller selbst prüfen und dokumentieren müssen, ob das Update eine Genehmigungsrelevanz hat. Nur wenn der Fahrzeughersteller der Auffassung ist, dass es sich um ein genehmigungsrelevantes Update handelt, wird ein neuer Genehmigungsprozess notwendig. Diese Entscheidung und Bewertung trifft aber immer der Fahrzeughersteller.

Können Sie ein Beispiel nennen?

K. Graef: Anwendung finden die zwei neuen UN-Regelungen schon beim neuen Level-3-System für autonomes Fahren, dem ALKS (Automated Lane Keeping System). Hierfür werden die Fahrzeughersteller sogar in die Pflicht genommen, Updates aufzuspielen, um die Cybersicherheit des Systems auch künftig noch gewährleisten zu können. Die Hersteller dürfen also nur Sicherheits-Updates durchführen. In dem Moment, in dem Funktionserweiterungen im Spiel sind, wäre es ein genehmigungsrelevantes Update. Der komplette Genehmigungsprozess müsste dann nochmals durchlaufen werden und auch nationale Zulassungsvoraussetzungen müssten zunächst geklärt werden.

Was ist, wenn ein Hersteller Funktionen ohne diese Genehmigung nachrüstet?

K. Graef: In Europa gibt es Marktüberwachungsbehörden, die überprüfen, ob Fahrzeuge der Genehmigung entsprechen. Hier können durchaus auch zugelassene Kundenfahrzeuge herausgesucht und überprüft werden. Die Überwachung wird inzwischen auch auf gesamteuropäischer Ebene durchgeführt, und zwar selbst dann, wenn das Fahrzeug ursprünglich das Genehmigungsverfahren in einem anderen Land durchlaufen hat.

Lassen sich Software-Updates bei der Hauptuntersuchung (HU) überprüfen?

K. Graef: Ja, das ist möglich. Eine Überprüfung auf Zustand, also die richtige Software-Nummer, gibt es schon für diverse Fälle. Software-Versionen mit unterschiedlichen Merkmalen der Software benötigen je nach zugeschalteter Funktion im Übrigen auch den Nachweis der Hochrüstung. So sieht es die StVZO in der Anlage 8e vor. Weiterhin werden derzeit auch überwachte

Kategorien von Software-Updates

Kategorie 1: Updates zur Wiederherstellung der Konformität mit der Typgenehmigung

Diese Kategorie von Updates wird beispielsweise im Falle eines Rückrufs aufgespielt, um die genehmigungskonforme Funktion des Fahrzeugs wiederherzustellen.

Kategorie 2: Updates ohne Änderung von sicherheits- oder typgenehmigungsrelevanten Funktionen/Systemen

Updates ohne Genehmigungsrelevanz umfassen Updates für Fahrzeugfunktionen, die keine Fahreigenschaften verändern und dadurch keine Genehmigungsrelevanz haben.

Kategorie 3: Updates zur Aktivierung zusätzlicher typgenehmigungsrelevanter Funktionen („Functions on Demand“)

Diese Kategorie umfasst Updates, die zusätzliche Funktionen im Fahrzeug nachrüsten. Die Hardware ist dabei schon ab Werk vorhanden und wird mittels Software-Update freigeschaltet. Das kann auch temporär sein.

Kategorie 4: Updates zur Aktivierung zusätzlicher typgenehmigungsrelevanter Funktionen, die noch nicht durch die erste Typgenehmigung abgedeckt sind

Zu dieser Kategorie zählen Updates, die Funktionen des Fahrzeugs dahingehend verändern, dass die ursprüngliche Genehmigung nicht mehr gültig ist. Dazu zählen beispielsweise Funktionen, wie unter Kategorie 3 beschrieben, welche zum Zeitpunkt des Inverkehrbringens des Fahrzeugs aber noch nicht genehmigt waren.

Kategorie 5: Updates wie in Kategorie 4, die aber zusätzlich zulassungsrelevante Daten ändern

Grundsätzlich wie Kategorie 4, jedoch werden zusätzlich die Daten des Fahrzeugs geändert, die in den Zulassungsdokumenten stehen.



Foto: Bosch

**Update ist nicht gleich Update:
Je nach Typ gelten andere Regeln**

te Rückrufe, wie im Fall des Dieselskandals, mittels HU-Adapter auf den richtigen Softwarezustand überprüft. Wenn die Software nicht dem gewünschten Stand entspricht, ist das ein erheblicher Mangel bei der Hauptuntersuchung.

Wie lässt sich die Sicherheit beim Aufspielen eines Software-Updates garantieren und wie lassen sich Manipulationen an der Software ausschließen?

K. Graef: Der Autohersteller muss im Rahmen seiner Produkthaftung auch die Sicherheit der Software-Updates gewährleisten. Nur weil ein Update nicht in der Werkstatt, sondern Over-the-Air stattfindet, muss es nicht unsicher sein. Auch ein

Zentralrechner im Auto heißt nicht automatisch, dass sich Software manipulieren lässt. Es muss aber sichergestellt sein, dass neben dem Fahrzeughersteller auch ein unabhängiger, berechtigter Dritter Zugang zu den Daten bekommt oder die Daten überprüfen kann. Hier sind wir bereits auf einem guten Weg, eine europaweite beziehungsweise über die UNECE gültige Lösung zu finden. Unklar ist aber noch, ob und wie Dritte, beispielsweise freie Werkstätten oder Teilehersteller, auf die Fahrzeugsoftware zugreifen oder Software aufspielen dürfen.

Herzlichen Dank, Herr Graef, für das Interview.

Alexander Junk