EUSTACCHIO

Die Tücken von Software-Updates in vernetzten Autos

„Over the air“ Software-Updates in vernetzten Autos sind nicht mit routinemäßigen Updates für Smartphones vergleichbar, sagt Technologie- und Industrieanwalt Andreas Eustacchio.

Technologie- und Industrieanwalt Andreas Eustacchio erklärt, dass es für Hersteller von Hardware und Software-Entwickler vor allem um die Frage nach der Sicherheitserwartung geht.

Bei Smartphones sind Software-Aktualisierungen die Regel. Bei IoT-fähigen Geräten und vernetzten Autos sind sie ebenfalls im Kommen. Was bedeutet das für die User?

ANDREAS EUSTACCHIO: Zunächst muss man deutlich zwischen *Updates* und *Upgrades* unterscheiden. Aus Nutzersicht ist der Vorteil reiner Updates auf den ersten Blick gar nicht wahrnehmbar. Denn Updates sollen immer auch den aktuellen Sicherheitsstandard widerspiegeln, um das Gerät ohne Funktionseinschränkungen und frei von Cyberangriffen weiter so nutzen zu können wie bisher. Davon klar zu unterscheiden sind Software-Upgrades, also über die Erhaltung der Funktion hinausgehende Verbesserungen, die dem Nutzer höheren Komfort bei der Verwendung von Produkten mit digitalen Inhalten geben. Das können Fahrassistenzsysteme in Autos sein, ein „intelligenter“ Kühlschrank, aber auch Zusatztools für die „smarte“ Fitness-Uhr. Aus Verkäufersicht stellen Upgrades immer auch den Versuch dar, bestehende Kunden an ihre Produkte zu binden. Updates dienen dagegen der Aufrechterhaltung der Funktion und sind dazu gedacht, neu erkannte Sicherheitslücken zu schließen.

Inwieweit ist diese Unterscheidung für Produkt- und Software-Entwickler rechtlich von Bedeutung?

Bislang konnten Nutzer von Produkten mit digitalen Inhalten nicht sicher sein, dass diese während der Vertragslaufzeit auch mit den notwendigen Updates versorgt werden. Gerade wenn die Nutzung eines Produkts von einem Update abhängt, kann das Fehlen der entsprechenden Software-Aktualisierung das Produkt in seiner ursprünglichen Funktion einschränken oder wertlos machen. Schon bisher konnte man darauf bestehen, diesen Gewährleistungsmangel durch ein Update zu beheben. Seit 1. Jänner 2022 gilt das Verbrauchergewährleistungs-Gesetz (VGG) und damit ausdrücklich eine Aktualisierungs-, also Update-Pflicht, und zwar unentgeltlich. Diese trifft Verkäufer beziehungsweise Händler, auch wenn die von ihnen vertriebenen Produkte im Zeitpunkt des Kaufs Software enthält, die dem Nutzer direkt von der Software-Firme bereitgestellt wird. Diese Aktualisierungspflicht gilt nicht nur für Geschäfte mit Verbrauchern (B2C), sondern auch für solche zwischen Unternehmern (B2B). Unternehmer können die Aktualisierungspflicht aber auch vertraglich ändern und ausschließen.

Für welche Dauer besteht diese Aktualisierungspflicht?

Zumindest für zwei Jahre nach der Übergabe des physischen Produkts. Das kann aber auch ein längerer Zeitraum sein. Das Gesetz spricht eher unbestimmt vom Zeitraum, den der Verbraucher unter Berücksichtigung der Umstände und der Art des Vertrages vernünftigerweise erwarten kann.

Was ist, wenn ein Nutzer keine Aktualisierungen will?

Da das Funktions-Update immer auch eine vertragliche Abweichung vom ursprünglichen Vertragsgegenstand darstellt, muss der Nutzer nach dem VGG darüber eigens in Kenntnis gesetzt werden und er muss dem Funktions-Update ausdrücklich und gesondert zustimmen. Verweigert er die Zustimmung, entfällt die Aktualisierungspflicht.

Warum sollte das jemand tun?

Eine vollkommen fehlerfreie Programmierung kann kein Software-Entwickler zusagen. Es ist nicht auszuschließen, dass gerade auch über ein Software-Update eine Fehlfunktion infiltriert und gerade erst deshalb ein Sicherheits-Update notwendig wird, Stichwort Hacking und Cybersecurity.

Wie sieht es bei Fahrzeugen mit softwarebetriebenen Assistenzsystemen, kurz „connected cars“ aus, deren Updates über die Sicherheit und damit über Leben und Tod entscheiden?

Bei sicherheitsrelevanter Software ist ein Update unabhängig von Gewährleistungs- oder vernünftigerweise zu erwartenden Nutzungszeiträumen immer zwingend erforderlich. Dazu gibt es allerdings keine ausdrückliche Gesetzesstelle. Dies ergibt sich vielmehr aus den unterschiedlichen gesetzlichen Bestimmungen zur Produktsicherheit, der Product-Compliance sowie der Produktbeobachtungspflicht, und zwar nicht nur gegenüber dem eigenen Vertragspartner in der B2B-Lieferkette, sondern gegenüber jedem Produktnutzer.

Was heißt das für Hersteller?

Ganz konkret, dass es zur Abwehr einer ernstzunehmenden Gefahr für Leib und Leben nicht ausreicht, Nutzern Software zum Zwecke der Sicherheitsaktualisierung bloß bereitzustellen, im Sinne einer Bereitstellungspflicht. Vielmehr kann Hersteller sogar eine Update-Durchführungspflicht treffen, wenn sie präventiv Schäden verhindern und spätere Haftungsfolgen mit hohen Schadenersatzzahlungen vermeiden wollen. Und diese Pflicht besteht unabhängig davon, ob sie selbst Vertragspartner der Nutzer ihrer Fahrzeuge sind oder nicht. Gerade bei Fahrzeugherstellern besteht ein direktes Vertragsverhältnis zum Fahrzeugnutzer aufgrund der Lieferkette in der Regel nicht.

Heißt das, dass Nutzer Sicherheits-Updates nicht verhindern können und diese dulden müssen?

Die Frage ist, welche Sicherheitserwartung Nutzer in ihre vernetzten Produkte haben dürfen. Fehlfunktionen oder Hackerangriffe sind heute nicht mehr ungewöhnliche Ereignisse, sondern eher schon zu erwarten. Dies gilt gerade für vernetzte Fahrzeuge, weshalb Sicherheits-Updates die Regel sein werden. Wenn also Hersteller eine Gefahr für Menschen nicht durch Warnungen oder sonstige Hinweise beseitigen können, wird ein Sicherheits-Update „over the air“ (OTA) als angemessen anzusehen sein, gerade wenn dies einen physischen Rückruf ersetzt. Dafür muss die Zustimmung des Nutzers nicht eingeholt werden. Ob ein OTA-Update daneben auch empfangstechnisch möglich ist, hängt in erster Linie von den zur Verfügung stehenden Schnittstellen zur Datenübertragung (etwa WLAN, Mobilfunk usw.) ab. Nutzern muss klar vermittelt werden, dass es um entsprechende Sicherheits-Updates geht. Verhindern oder blockieren Nutzer diese Updates bewusst oder deaktivieren sie die Übertragung, so kann im Schadensfall der Hersteller nicht in die Haftung genommen werden. Das ist wie mit dem Aufruf eines Herstellers zum Rückruf seiner Produkte in der analogen Welt. Kommt jemand dem nicht nach, kann er sich beim Hersteller für dadurch verursachte Schäden auch nicht schadlos halten.

Wann hätte ein Nutzer wegen eines Software-Updates Schadenersatzansprüche?

Zum Beispiel, wenn es durch ein Software-Update zur Einschränkung anderer Funktionen desselben Produkts kommt. Ein Fall des Landgericht München vom 13. September 2021 verdeutlicht dies: Ein in der Höhe verstellbarer Tesla (15 cm nach oben und unten) war laut Kaufvertrag mit einem „Enhanced Autopilot“ um 6000 Euro ausgestattet, zum Gesamtkaufpreis von 154.430 Euro. Diese Funktion musste gesondert heruntergeladen werden. Als der Nutzer den Download-Button betätigte, ging er davon aus, dass es sich um das Update eben dieses Autopiloten handelte, stattdessen wurde dadurch die Funktion der Höhenverstellbarkeit eingeschränkt, was für den Nutzer überraschend war. Nach Ansicht des Gerichts hätte dieser über den genauen Inhalt und die Folgen des Updates vorab aufgeklärt werden müssen. Mit einem routinemäßigen Software-Update für ein Smartphone ist dies nicht vergleichbar, so das Gericht, weil mit dem Update eine andere bestehende Funktion außer Kraft gesetzt wurde. Der Käufer hatte, weil außerhalb der Gewährleistungsfrist, einen Schadenersatzanspruch auf Rückabwicklung des Kaufvertrages, weil die Höhenverstellbarkeit nicht mehr rückgängig gemacht werden konnte. Daran änderte nichts, dass die Software für den Download nicht vom Verkäufer, sondern direkt von der Tesla Inc. zur Verfügung gestellt wurde. Diese wurde als Erfüllungsgehilfe des Händlers angesehen

Durch Systemeingriffe können Daten auch widerrechtlich abgesaugt werden. Wer hat an diesen eigentlich das Nutzungsrecht?

Wenn die von einem Fahrzeug generierten Daten in Verbindung mit dem Nummernschild, der Fahrzeugidentifikationsnummer oder gerätespezifischen Identifikationsnummern Rückschlüsse auf eine Person zulassen, sind dies personenbezogene Daten und damit nach der Datenschutz-Grundverordnung (DSGVO) geschützt. Nur mit Zustimmung des Betroffenen dürfen sie verarbeitet werden. Dennoch wissen die meisten Menschen gar nicht, ob und welche Daten Autohersteller von ihnen und ihrem Auto verwenden. Dies gilt auch für eine Reihe von Daten, die zwar nicht personenbezogen sind, aber vom Fahrzeug generiert werden. In der Praxis wird dem Nutzer oder der markenfremden Werkstatt der Zugriff darauf verweigert. Mit dem Entwurf des „Data Act“ der EU-Kommission sollen Hersteller diese Daten teilen und auch Dritten unentgeltlich zur Verfügung stellen müssen.

FOTO: DANIEL NOVOTNY

AUTO MOTIVE LAW
EUSTACCHIO
Rechtsanwälte • Attorneys at Law

EUSTACCHIO Rechtsanwälte
Währinger Straße 26
1090 Wien
Tel.: +43/(1) 319 97 00
office@eustacchio.com
eustacchio.com

Diese Seite entstand mit finanzieller Unterstützung von EUSTACCHIO.