Vernetzte Autos und Datenökonomie

Bei der Entwicklung von Produkten und Lösungen im Automotive-Markt sollte Datenökonomie das oberste Prinzip sein. Die sparsame Nutzung von Kunden- und Fahrzeugdaten kommt dabei nicht zuletzt den OEMs selbst zugute. Das Marktforschungsunternehmen Gartner prognostiziert, dass bis 2020 rund 250 Millionen vernetzte Fahrzeuge weltweit auf den Straßen unterwegs sein werden. Kundenbefragungen machen jedoch deutlich, dass die Nutzer bei allen Vorteilen, die ihnen diese Vernetzung bietet, sehr besorgt über die Konsequenzen für ihre Privatsphäre sind.

Daten gelten heute als eigene Währung. Die Möglichkeiten zur Monetarisierung von Kundendaten sind fast endlos und reichen von der Vorhersage freier Parkplätze über die Anreicherung von Kartendaten bis hin zu Innovationen von Fahrerassistenzfunktionen. Aus der Verbindung von Fahrzeugsensoren und cloudbasierten Analysemethoden und Diensten ergeben sich eine Vielzahl möglicher Anwendungen, die sich an unterschiedliche Zielgruppen richten – den OEM selbst, etwa zur Weiterentwicklung seiner Produkte, Zulieferer aller Ebenen, Vertrags-Händler und -Werkstätten, und nicht zuletzt den Endkunden, also Fahrer oder Fahrzeughalter. Andererseits ist das Vertrauen ihrer Kunden für Autohersteller im harten Konkurrenzkampf ein entscheidender Faktor.

Dies stellt Unternehmen und Serviceanbieter vor ein Dilemma: Auf der einen Seite verspricht die Nutzung von Daten neue Geschäfts- und Erlösmodelle, auf der anderen Seite hätte eine Enttäuschung des Kundenvertrauens oder gar ein Datenschutz-Skandal katastrophale Auswirkungen auf das Image des Unternehmens und zudem gravierende juristische Konsequenzen. Die Problematik in diesem Spannungsfeld verschärft sich noch, weil neue Analysemöglichkeiten aus dem „Big Data"-Bereich vermeintlich anonymisierte Daten leicht wieder einzelnen Personen zuordnen können. Beim Umgang mit Kundenidentitäten, Bewegungsdaten und Kommunikations-Metadaten müssen Autohersteller und Anbieter von Datendiensten diese Problematik im Blick behalten. Empfehlenswert ist eine Strategie der Selbstbeschränkung (Bild 1).

Anonymisierung komplexer als gedacht

Die Vorstellung, Bewegungsprofile, Geo-Lokalisierungen oder „Floating Car Data" ließen sich etwa durch Entfernung persönlicher Daten wie Namen oder Kundennummern ausreichend pseudonymisieren, ist bereits mit dem Blick auf heute verfügbare Analysemethoden zum Scheitern verurteilt. Regelmäßige Fahrten zwischen Zuhause und dem Arbeitsplatz ermöglichen mit geringem Aufwand die nachträgliche Zuordnung von Bewegungsdaten zu einer individuellen Person. Selbst isolierte Diagnosedaten können durch „Fingerabdrücke" wieder mit einem einzelnen Fahrzeug und somit seinem Fahrer verbunden werden. Diese Beispiele ließen sich beliebig fortsetzen – die Trennung von Nutzdaten, die für bestimmte Applikationen oder Analysen einen hohen Wert darstellen, und ihrer „Besitzer" oder „Verursacher" stellt eine

Bild 1: Motivationen zur sparsamen Nutzung von Kunden- und Fahrzeugdaten. (© Elektrobit)

nymisierte, pseudonymisierte oder mit „entschärften" Zeitstempeln gekennzeichnete Daten wieder einzelnen Personen zuordnen.

Breites Spektrum an Risiken

Nun stellt sich vielleicht die Frage, worin denn die Gefahr bei einem solchen nachträglichen Aufheben von Datenschutzmaßnahmen besteht. Dazu sollten Verantwortliche das Spektrum möglicher Bedrohungen im Auge behalten. Es beginnt bereits bei Geschäfts- und Kooperationspartnern, die möglicherweise unter einer anderen Jurisdiktion stehen oder weniger weitreichende Datenschutzmechanismen in ihrem Unternehmen implementiert haben. So liegt etwa für manche US-Unternehmen die weitreichende Analyse personenbezogener Daten nicht nur im Kern ihres Geschäftsmodells, sie unterliegen in ihrem Heimatland auch viel schwächeren Datenschutzbestimmungen, als sie etwa in Europa gültig sind. Eine unter diesen

größere Herausforderung dar, als man auf den ersten Blick annehmen könnte.

Soll der Daten- und Persönlichkeitsschutz des einzelnen Kunden gewährleistet bleiben, muss Datensicherheit beziehungsweise Datenökonomie deshalb von vornherein beim Design einer Anwendung berücksichtigt werden. Eine verbreitete Strategie ist etwa die Trennung von Authentisierung und Dienstleistung – ein online bereitgestellter Dienst weiß dann nur, dass an ihn eine berechtigte Anfrage gestellt wurde, aber nicht, wer sich dahinter verbirgt. Doch Metadaten wie etwa die IP-Adresse können den Nutzer trotzdem verraten – sie müssen also entfernt werden. Weiter verbessern lässt sich die Anonymisierung, indem keine kompletten Routen aufgezeichnet und gespeichert werden, sondern nur einzelne „zerhackte" Segmente daraus. Bei Zeitstempeln gibt es den Ansatz, das Tagesdatum komplett zu entfernen, und nur Stunden und Minuten zu speichern. Die Nutzung der Daten in Applikationen – beispielsweise die Erzeugung von Auslastungsprofilen für Streckenabschnitte – muss dann von vornherein so konzipiert werden, dass sie mit diesen unscharf gemachten Daten auskommt (Bild 2).

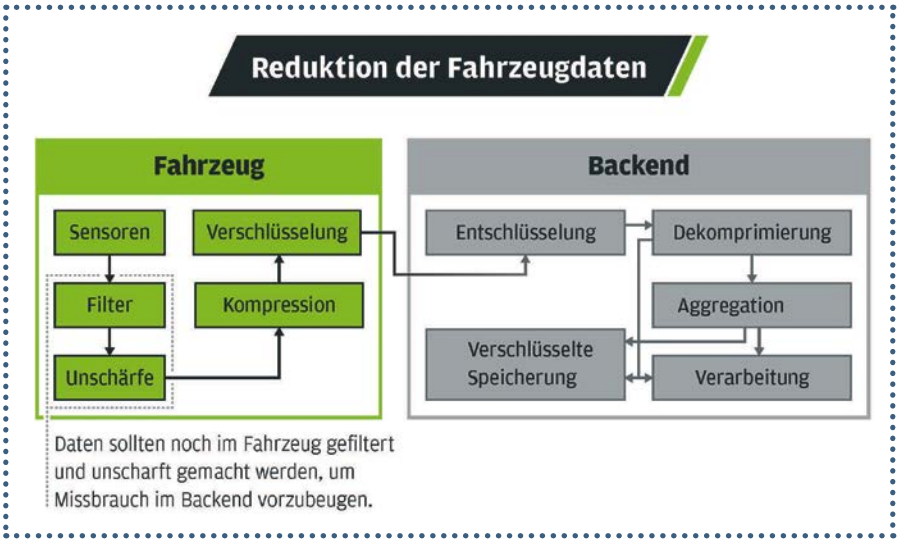

Bild 2: Die Reduktion der Daten bereits im Fahrzeug verbessert die Sicherheit. (© Elektrobit)

Dennoch sollte Ingenieuren und Entwicklern bewusst sein, dass sie mit solchen Maßnahmen lediglich das Sicherheitsniveau verbessern. Der Leitspruch von Datenschützern „Absolute Sicherheit gibt es nicht" mag sich abgedroschen anhören, ist im Kern jedoch zutreffend. Wer ausreichend Aufwand und Ressourcen investiert, kann auch zerhackte, ano-

Vorzeichen stattfindende Nutzung von Daten, die beispielsweise ein deutscher Hersteller von seinen Kunden erhebt, könnte aus der Sicht europäischer Juristen bereits ein Missbrauch sein. Dies hätte nicht nur ernsthafte Konsequenzen für den Ruf des Unternehmens, sondern könnte empfindliche rechtliche Folgen nach sich ziehen. Die europäische Datenschutz-Grundverordnung sieht beispielsweise Geldbußen bis zu 20 Millionen Euro oder bis zu vier Prozent des gesamten weltweit erzielten Jahresumsatzes im vorangegangenen Geschäftsjahr vor.

Nicht minder bedrohlich ist die Aussicht, dass personenbezogene Daten etwa durch Hackerangriffe in die falschen Hände geraten könnten – die vergangenen Jahre zeigten Beispiele mehrerer bekannter Unternehmen, die Opfer großer Datendiebstähle wurden. Diese Risiken sind noch schwerer »

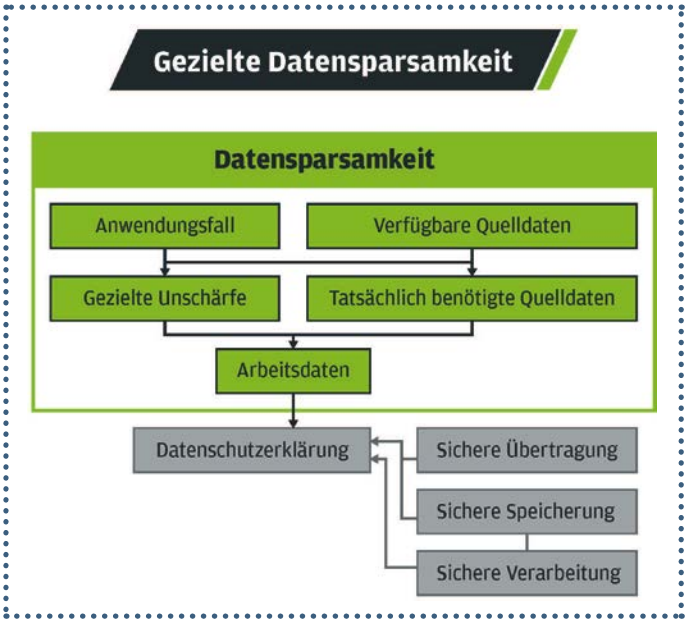

Bild 3: Der Datenschutz sollte bei der Entwicklung von Diensten und Anwendungen von vorherein eine wichtige Rolle spielen. (© Elektrobit)

zu bewerten, wenn man bedenkt, dass Angriffe und Datendiebstähle zu einem hohen Anteil durch eigene Mitarbeiter oder aus dem nächsten Umfeld des Unternehmens verursacht werden. Der Branchenverband Bitkom berichtet in seiner 2015 veröffentlichten Studie „Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz im digitalen Zeitalter", dass bei Fällen aus den Jahren 2013 und 2014 bei insgesamt 550 betroffenen Unternehmen die mutmaßlichen Täter zu 52 Prozent aktuelle oder ehemalige Mitarbeiter sind und zu 39 Prozent dem engeren Umfeld des Unternehmens entstammen. Organisierte Kriminalität, Hobby-Hacker und ausländische Geheimdienste nehmen demgegenüber einen erheblich kleineren Anteil ein. Abgesehen von direkten finanziellen Schäden wie Schadensersatzansprüche und Bußgelder, kann der durch Aufdeckung solcher Fälle entstehende Reputationsverlust langfristig noch viel größere Schäden verursachen.

Vorsicht vor Rechteeinräumung „auf Vorrat"

Doch auch diese Folgen sind nur ein Teilaspekt der Problematik. Auch die rechtmäßige und IT-technisch abgesicherte Nutzung von Kundendaten birgt rechtliche wie auch strategische Fußangeln. Grundsätzlich verlangen das Bundesdatenschutzgesetz und die entsprechenden europäischen Richtlinien, dass die Kunden genau darüber informiert werden, welche Daten zu welchem Zweck gesammelt werden. Diese Information erfolgt üblicherweise in Benutzervereinbarungen, die vom Kunden bestätigt oder etwa als Bestandteil eines Kauf- oder Leasingvertrags gegengezeichnet werden müssen. Hier sollten Anbieter zum eigenen Schutz deutlich formulieren, auf welcher technischen Grundlage sie welche Dienste anbieten. Ein Zielkonflikt ergibt sich jedoch im Hinblick auf künftige neue Geschäftsmodelle oder Erweiterungen bestehender Dienste. Jeder Dienst, der online angeboten wird, birgt das Risiko, dass die dabei gesammelten Daten für andere Zwecke verwendet werden, als für die, denen die Nutzer zugestimmt haben. Darunter fällt auch die Weitergabe der Daten an Dritte ohne explizite Einwilligung. Gründe dafür reichen von Unwissen beim Servicebetreiber über Schlamperei und Einsparungen bei der Sicherheit bis hin zu Geschäftsmodellen, die den Kundeninteressen widersprechen.

Besteht die Möglichkeit, dass für künftige Anwendungen oder Geschäftsmodelle zusätzliche Daten benötigt werden, könnten gerade auch sorgfältig arbeitende Unternehmen in Erwägung ziehen, sich in den Nutzungsvereinbarungen von vornherein weitreichende Rechte zu sichern. Doch auch dieses Vorgehen birgt hohe Risiken – zum einen juristisch, denn die Rechtsprechung gerade in Deutschland ist in Sachen Datenschutz oft eher restriktiv. Zum anderen für das Image des Unternehmens – erinnert sei etwa an den Skandal um einen namhaften koreanischen TV-Hersteller, der sich in den Nutzungsbedingungen seiner „Smart TVs" das Recht einräumte, jedes vor dem Gerät gesprochene Wort aufzuzeichnen und in seinen Rechenzentren zu analysieren. Es ist leicht auszumalen, welche Folgen etwa ein ähnliches Ansinnen im Zusammenhang mit cloud-basierter Spracherkennung im Auto haben würde.

Rechtssicherheit und Kundenschutz im Fokus

Die Abwägung von Datenschutzanforderungen und datenbezogenen Geschäftsmodellen bleibt somit ein ständiger Prozess. Die einzige wirklich sichere Art zu verhindern, dass Daten in falsche Hände gelangen, ist dafür zu sorgen, dass sie gar nicht erst entstehen. Welche Handlungsempfehlungen ergeben sich daraus?

Wie eingangs bereits erwähnt, erfordert es einen nicht unbeträchtlichen technischen Aufwand, Daten so zu anonymisieren oder unscharf zu machen, dass sie ein erhöhtes Schutzniveau bieten. Unternehmen sollten diesen Aufwand als Investition in ihren Ruf und künftige Kundenbeziehungen betrachten. Beim Design von Diensten und Anwendungen sollte der Datenschutz von vorherein eine zentrale Rolle einnehmen. Die Applikationen und Lösungen sollten so ausgelegt werden, dass sie nur gerade so viele Daten nutzen, wie für das konkrete Angebot unbedingt nötig. Eine Erfassung und Speicherung von Daten „auf Vorrat" beziehungsweise „auf Verdacht" ist hoch problematisch und sollte unbedingt vermieden werden. Unternehmen sollten mit firmeninternen Richtlinien alle Aspekte des Umgangs mit und der Nutzung von Kundendaten detailliert regeln (Bild 3). Dazu zählt auch, einen Datenschutzbeauftragten zu bestimmen und diesen mit ausreichenden Vollmachten auszustatten. Die Kunden werden solche Bemühungen mit anhaltender Markenloyalität danken. ■ (oe)

» **www.elektrobit.com**

Sebastian Bär ist für die Software-Architektur der Abteilung Connected Car bei Elektrobit verantwortlich.