Titelthema Sicherheit und Datenschutz

Datenschutzalptraum VBB-fahrCard

aus SIGNAL 05/2013 (November 2013), Seite 4-5 (Artikel-Nr: 10003157)
Berliner Fahrgastverband IGEB

Fahrkarte mit Facebook-Status Vertrauen ist gut, Kontrolle ist besser. Deshalb muss man als Kunde nach dem Kauf der Fahrberechtigung einen Nachweis, auch »Fahrkarte» genannt, mit sich führen.

Diese wird vor, während oder auch mal nach der Fahrt von Mitarbeitern der Verkehrsunternehmen kontrolliert. Für das Unternehmen reicht das Wort des Kunden, er habe für die Fahrt bezahlt, also nicht aus.

Nun hat sich die Welt weiterentwickelt, technisiert, digitalisiert. Das macht auch vor den Fahrausweisen nicht halt. Statt Papierschnipsel durch die Gegend zu tragen, soll die Fahrberechtigung nun also elektronisch gespeichert werden. Das ist ersteinmal auch nicht schlimm. Trotzdem stellt sich die Frage: Was wird da außer der reinen Fahrberechtigung noch gespeichert? Persönliche Daten?

Bereits eine ID, eine eindeutige Identifikationsnummer, reicht aus, um die Frage nach dem Datenschutz aufzuwerfen. Immer wenn eine Überprüfung durchgeführt wird, wird die ID fleißig ausgetauscht. Gemeinsam mit den Informationen, wann, wo und wie häufig diese ID ausgelesen wurde, könnte sie eine bei allen Unternehmen äußerst begehrte Informationsquelle bilden. Denn bereits nach wenigen Kontrollpunkten ließe sich damit schon ein ziemlich gutes Fahrprofil über den Eigentümer erstellen.

Hinzu kommt, dass diese ID keinesfalls anonym ist. Sie ist vielmehr eine Kartennummer. Abgelegt im System und eindeutig Ihrem Abo und Ihrer Person zugeordnet.

Nur ein Horrormärchen?

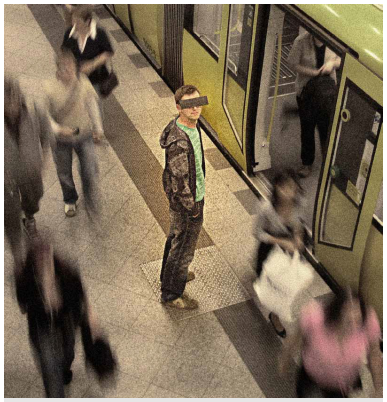
In der VBB-Werbebroschüre ist zum Thema Sicherheit Folgendes zu lesen:

»[...] Kann mein Verkehrsunternehmen oder der VBB nun alle meine Fahrten nachverfolgen?

Nein, es ist weder technisch noch organisatorisch möglich, sogenannte Bewegungsprofile auf der Karte oder im System zu speichern. [...]»

Diese Aussage ist schlichtweg falsch! Die Karten basieren auf der sogenannten VDV-Kernapplikation E-Ticket. In deren Spezifikationen sind ausdrücklich Datenfelder für allerlei persönliche Daten sowie einer gesamten Fahrtenhistorie vorgesehen - für die Karte, für die Schnittstellen zum Auslesen und Schreiben sowie selbstverständlich vor allem für das Hintergrundsystem.

»[...] Bei der Kontrolle wird Ihre persönliche Chipkartennummer nur gegen eine Sperrliste geprüft, um festzustellen, ob Ihre Fahrtberechtigung noch gültig ist. Es werden keine personenbezogenen Daten gespeichert. [...]»



Der Fahrgast im Fokus. Auf ihn sind Kameras gerichtet. Seine Daten werden gesammelt. Aber wozu? Und welche Probleme und Gefahren sind damit verbunden? Unser Themenschwerpunkt Sicherheit und Datenschutz. (Foto: Raul Stoll, Bearbeitung: Holger Mertens)

Sie benutzen die neue elektronische »fahrCard»? Gut! Jedoch nicht für Sie, aber für die Verkehrsunternehmen. Denn anonym ist sie wirklich nur für den Nutzer. (Foto: IGEB)

Mit diesen stationären Geräten in Kundenbüros soll der Fahrgast kontrollieren können, was auf seiner Fahrcard gespeichert ist. Die Felder »Besitzer« und »Geboren« waren in einer früheren Version nicht zu sehen. Eine ID ist mit Sicherheit vorhanden, wird aber nicht angezeigt. Was ist außer diesen Feldern noch gespeichert? (Foto: IGEB)

Unwahrscheinlich. Denn hier geht es ums Geld. Die Karte kann vom Verkehrsunternehmen so hoch verschlüsselt werden, wie es will. Das schützt aber vor Clonen nicht. Clone sind 1:1-Kopien der verschlüsselten Karten, die beim Auslesen durch Kontrollgeräte nicht vom Original unterschieden werden können.

Um Clone zu erstellen, muss man keine Verschlüsselung knacken. Unbeschriebene Karten-Rohlinge beispielsweise aus Fernost übernehmen den gesamten verschlüsselten Inhalt samt Karten-Produktions-ID von einer beliebigen Original-Karte. In Anbetracht des hohen Fahrkartenwertes einer Jahreskarte ist der Anreiz für solche kriminellen Handlungen durchaus gegeben.

Doch wie kann ein Verkehrsunternehmen dem vorbeugen? Da die Karten äußerlich keinerlei Sicherheitsmerkmale tragen, ist die optische Prüfung bei Kontrollen ungeeignet. Da hilft nur, Karten-IDs bei jedem Lesevorgang mit Ort und Zeit zu speichern, daraus ein Bewegungsprofil zu erstellen und bei ungewöhnlich häufiger Nutzung oder unmöglichem Fahrverhalten auf mehrere Karten mit derselben ID zu schließen und diese dann zu sperren. Betroffen sind dann sowohl die Kopien als auch das Original, dessen Eigentümer nicht einmal wissen muss, dass seine Karte für illegale Kopien verwendet wurde. Das Auslesen der Karten erfolgt schließlich per Funk.

Das allein könnte aber erklären, warum ungültige Karten bei der Kontrolle sofort eingezogen werden. Und warum abgelaufene Karten vom Kunden wieder zurück geschickt werden müssen, obwohl Aufwand und Porto die Kosten der Karte weit übersteigen. Es erklärt auch, warum der Verlust der Karte beim Kunden mit jeweils unverschämten 20 Euro (10 beim ersten Mal) zu Buche schlägt.

»[...] Die Daten auf dem Chip sind grundsätzlich nur von Mitarbeitern der Verkehrsunternehmen mit speziellen Lesegeräten lesbar. [...] Kunden können in Verkaufsstellen die auf dem Chip gespeicherten Daten an speziellen Kundeninformationsterminals (Infoterminals) auslesen. [...]»

Und das ist ein riesiges Problem. Durch die Verschlüsselung ist es dem Fahrgast nicht möglich, ungefiltert auf die Datensätze auf der Karte zu schauen. Was man davon sehen kann und was nicht, obliegt immer der vollen Kontrolle der Unternehmen.

Vertrauensfrage

Doch kann man den Verkehrsunternehmen trauen? Zumindest Skepsis ist angebracht. In der Diskussion um Beibehaltung oder Abschaffung des ständigen Buskneelings argumentierte die BVG teilweise mit nicht nachvollziehbaren Angaben wie der Behauptung, es gäbe keine einzige Beschwerde dazu, obwohl die IGEB von mehreren Beschwerden wusste. Als unredlich empfanden viele Fahrgäste auch eine BVG-Fahrgastbefragung, deren Ergebnisse die BVG als Votum der Berliner gegen Polstersitze und für Hartschalensitze in der U-Bahn wertete, obwohl bei der Umfrage ausschließlich Hartschalensitze zur Auswahl standen.

Kann man den Unternehmen also glauben, wenn sie behaupten, es werden mithilfe der Fahrcard keinerlei personenbezogene Daten erhoben, obwohl das möglich ist? Werden sie sich auch einer Erhebung durch Polizei oder Verfassungsschutz widersetzen

(dürfen)? Wer kontrolliert die Verkehrsunternehmen? Die Fahrgäste können es nicht überprüfen. Und das macht uns Sorge.

Die FahrCard-Probleme im Überblick **Verschlüsselung der Karte**

Alle Unternehmen können die Daten auf der Karte unkontrolliert lesen und schreiben. Kriminelle müssen für ihre Machenschaften die Verschlüsselung nicht knacken. Der einzige, der durch die Verschlüsselung ausgesperrt wird, ist der Kunde. Bleibt die Frage: Wozu? Üblich wäre eigentlich, die Daten klar zu speichern und zusätzlich eine verschlüsselte Kontrollnummer, die die Richtigkeit der Daten belegt.

Speicherung von IDs bei Kontrollen

Falls die (eindeutig einer Person zuordenbaren) Kartennummern systembedingt als Bewegungsprofil vorliegen müssen, um Kartenkopien bekämpfen zu können, wer hindert die Unternehmen dann am letzten Schritt, diese Information personenbezogen zu verwenden? Die Daten sind da, die Versuchung ist groß und eine Kontrolle nicht vorhanden.

Intransparenter Datenaustausch

Bei jedem Datenaustausch zwischen Karte und Lesegerät können beliebig Daten gelesen, geschrieben und gelöscht werden, ohne dass einer der Beteiligten etwas davon mitbekommen muss. So ließe sich über Nacht eine neue Eigenschaft wie beispielsweise »guter/schlechter Kunde» einführen.

Intransparente Infrastruktur

Selbst wenn auf der Karte außer der ID nichts weiter gespeichert werden würde, so ließen sich weitere Daten auf den Kontrollgeräten mitführen. Beispielsweise könnte man dem Kontrolleur beliebige Details über den Kunden anzeigen, die zur gelesenen Karten-ID passen. »Raucher», »Querulant», »nimmt gern Schwarzfahrer mit» ... Diese Reihe ließe sich beliebig fortsetzen.

Der VBB informiert seine Kunden in einer Broschüre folgendermaßen *»[...]* **Welche Daten werden auf der VBB-fahrCard gespeichert?**

Auf der VBB-fahrCard werden nur Daten gespeichert, die bisher auch auf dem Papierticket oder der Kundenkarte enthalten sind. Bei unpersönlichen Abonnements werden das Tarifprodukt, der tarifliche Geltungsbereich, die Gültigkeit und die Kartennummer gespeichert. Bei persönlichen Abonnements kommen Ihr Name sowie der Aufdruck eines Lichtbildes hinzu. Kundenkarten sind somit nicht mehr notwendig und entfallen. Über die gespeicherten Daten werden Sie beim Versand der VBB-fahrCard von Ihrem Verkehrsunternehmen informiert. Darüber hinaus haben Sie die Möglichkeit, sich die Daten auf Ihrer VBB-fahrCard in ausgewählten Kundenbüros durch Kundenbetreuer anzeigen zu lassen oder diese an

Kundeninformationsterminals, kurz Infoterminals, selbst auszulesen. Bei Namen werden dabei ggf. nur die ersten zwölf Zeichen angezeigt. Eine Zusammenstellung aller Kundenbüros, in denen Sie rund ums Thema VBB-fahrCard beraten werden, sowie eine Übersicht aller verfügbaren Infoterminals finden Sie unter VBB.de.

Kann mein Verkehrsunternehmen oder der VBB nun alle meine Fahrten nachverfolgen?

Nein, es ist weder technisch noch organisatorisch möglich, sogenannte Bewegungsprofile auf der Karte oder im System zu speichern. Bei der Kontrolle wird Ihre persönliche Chipkartennummer nur gegen eine Sperrliste geprüft, um festzustellen, ob Ihre Fahrtberechtigung noch gültig ist. Es werden keine personenbezogenen Daten gespeichert. Die (((eTicket-Systeme erfüllen die Anforderungen des Datenschutzes der Länder sowie des Bundes und sind mit dem Berliner Beauftragten für Datenschutz und Informationsfreiheit sowie dem Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg abgestimmt.

Können Dritte beim Auslesen der Daten auf dem Chip (z. B. im Verlustfall) Zugriff auf persönliche und/oder Kontodaten erlangen?

Die Daten auf dem Chip sind grundsätzlich nur von Mitarbeitern der Verkehrsunternehmen mit speziellen Lesegeräten lesbar.

Bei persönlichen Zeitkarten wird der Name des Karteninhabers auf der VBB-fahrCard aufgedruckt und elektronisch auf dem Chip hinterlegt.

Ein Zugang durch Dritte zu weiterführenden persönlichen Daten und zu Kontodaten durch Auslesen der Daten auf dem Chip ist nicht möglich, da diese nicht auf der Karte hinterlegt sind. Kunden können in Verkaufsstellen die auf dem Chip gespeicherten Daten an speziellen Kundeninformationsterminals (Infoterminals) auslesen. [...]»

Dieser Artikel mit allen Bildern online:
http://signalarchiv.de/Meldungen/10003157.