Sicherheitsrisiko Bordkarte

Daten von Flugpassagieren sind schlecht geschützt

Bordkarten und Gepäckanhänger sollte man stets gut hüten und nach dem Flug lieber vernichten statt sie unachtsam wegzuwerfen. Aufgedruckte Informationen und der Barcode erlauben Fremden sehr leicht Zugriff auf Ihre persönlichen Daten.

Von Urs Mansmann

Die Zeit der Check-in-Schalter am Flughafen läuft allmählich ab. Der Check-in wird von immer mehr Passagieren online erledigt. Letztlich geht es dabei nur um die Erfassung persönlicher Daten, vor allem Wohnort, Geburtsdatum und die Nummer des Ausweisdokuments. Die Bordkarte kann man sich selbst ausdrucken, das Schalterpersonal überprüft nur noch Identität und Reisedokumente und nimmt das Gepäck entgegen.

Die Daten der Reisenden sind dabei extrem schlecht geschützt. Bei der Flugbuchung laufen sie in eines oder mehrere dreier große Systeme: Amadeus, Sabre und Travelport. Welches zum Einsatz kommt, hängt davon ab, welchem der Systeme Airlines und Reisebüro angeschlossen sind.

Diese Datenbanken stammen aus den 70er- und 80er-Jahren, was man an Auszügen aus der Datenbank erkennt: Dort gespeicherte Tarifbeschreibungen und Flugtickets bestehen stets nur aus Text, ohne Groß- und Kleinschreibung, ohne Formatierung, dafür gespickt mit unverständlichen Kürzeln, die sich nur dem Eingeweihten erschließen, denn die Speicherung erfolgt seit jeher mit sechs Bit pro Zeichen. Zwar gibt es inzwischen Buchungssysteme, die diese Daten übersichtlich in einer grafischen Benutzeroberfläche darstellen, aber die Grundstruktur der Datenbank ist unverändert geblieben.

In der Infrastruktur fehlen schon immer grundlegende Sicherheitsmechanismen zum Datenschutz und zur Sicherung des Zugriffs. Auf dem letztjährigen CCC-Kongress (33C3) hielten die Sicherheitsexperten Karsten Nohl und Nemanja Nikodijevic zu diesem Thema einen vielbeachteten Vortrag (siehe ct.de/y6r7). Die Problematik hat sich aber offenbar noch nicht herumgesprochen, denn immer noch posten viele Flugpassagiere Fotos ihres Boarding-Passes und ermöglichen damit Fremden Zugriff auf viele persönliche Informationen.

Name als Passwort

Der Zugriff auf beliebige Flugdaten, den PNR (Passenger Name Record), ist denkbar einfach: Bei der Ausstellung des Tickets erhält der Flugpassagier einen sechsstelligen alphanumerischen oder Buchstaben-Code. Über spezielle Service-Angebote, beispielsweise CheckMyTrip (Amadeus), ViewTrip (Travelport) oder Virtually There (Sabre) kann jeder die wichtigsten Eckdaten eines Tickets abfragen, wenn er diese Informationen hat.

Mit diesem Zugriff lassen sich auch Flugbuchungen bei der Airline nachbearbeiten, beispielsweise für den Online-Check-in, für die Buchung von Menüs oder besonderen Sitzplätzen. In diesem Fall reichen die Buchungsnummer und der Nachname für den Login; nur in wenigen Fällen werden weitere Daten wie die E-Mail-Adresse oder das Geburtsdatum abgefragt, die ein Angreifer aber leicht in Erfahrung bringen kann.

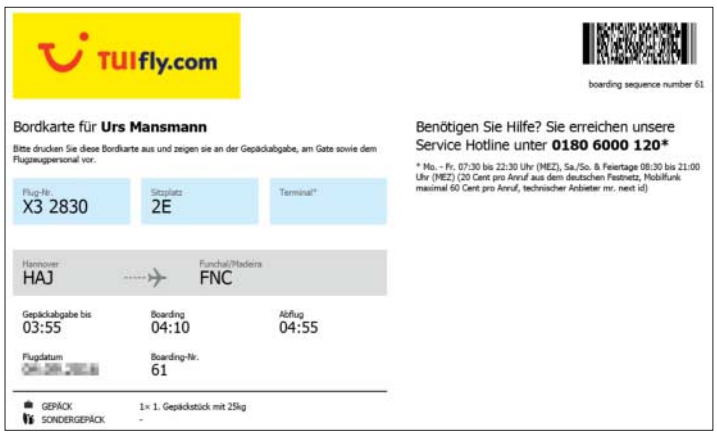
Angreifer können dann alle hinterlegten Informationen abrufen, also zunächst einmal die Flugdaten für den Hin- und gegebenenfalls den Rückflug – und das von allen Passagieren, die in der Buchung enthalten sind. Außerdem sind unter Umständen auch weitere Daten wie Anschrift, Telefonnummern, E-Mail-Adressen und Kreditkartendaten und Reisepassdaten einsehbar. In den Datenbanken ist auch erfasst, von welcher IP-Adresse aus die Buchung erfolgte. Menü-Sonderwünsche erlauben Rückschlüsse auf die Religionszugehörigkeit oder Krankheiten. Sogar das Umbuchen oder Stornieren ist unter Umständen auf den Seiten der Airline durch jeden möglich, der die Daten von der Bordkarte hat. Bei den Reisebüros hingegen läuft der Login meistens über eine interne Buchungsnummer oder einen separaten Kunden-Account, deren Daten nicht auf dem Boarding-Pass auftauchen.

Datendiebstahl vermeiden

Die Airlines wissen offenbar um den schlechten Schutz der Daten und drucken deshalb die Buchungsnummer in vielen Fällen nicht mehr auf die Bordkarte. Enthalten ist sie aber dennoch – in dem ebenfalls stets aufgedruckten und unverschlüsselten Matrixcode, denn beim Boarding muss ja eine Zuordnung zur Flugnummer erfolgen. Der lässt sich mit dem Smartphone per App leicht entziffern.

Damit Fremde keinen Zugriff auf Ihre Daten erhalten, sollten Sie auf gar keinen Fall Fotos von Boardingpässen oder Gepäckanhängern in soziale Medien stellen, in denen der PNR-Code, die Ticketnummer oder der Matrixcode lesbar sind. Nach dem Flug sollten Sie diese Dokumente sorgfältig vernichten und nicht achtlos wegwerfen – vor allem nicht am Flughafen. *(uma@ct.de)* c't

Video vom 33C3: ct.de/y6r7



Obwohl die Buchungsnummer nicht im Text auftaucht, ist sie im PDF-417-Code auf der Bordkarte enthalten.