

Die Bordkarte als Authentifikationsmittel bei Flugreisen

Mariia Astrakhantceva¹, Bettina Hübscher², Günter Karjoth³

Abstract: Mobile Technologien und das Web sind omnipräsent. Auch die Luftfahrtbranche setzt auf die Buchung über das Internet. Diese Angebote erhöhen nicht nur die Benutzerfreundlichkeit, optimieren den Abflugprozess und ersparen Millionen Euro an Kosten, sondern enthalten auch Gefahren – für Passagiere wie Fluglinien. Veröffentlicht jemand das Foto einer Bordkarte auf dem Internet, kann die darauf abgedruckte Information verwendet werden, um beispielsweise den Rückflug zu annullieren. Diese Gefahr ist vielen Passagieren nicht bewußt. Die Möglichkeit dieses Angriffs besteht nicht nur durch das Wissen über die Information auf der Bordkarte, sondern auch durch eine schwache Authentifizierung auf Seite der Fluglinie. Dieser Artikel beschreibt die technischen Grundlagen, diskutiert die rechtlichen Aspekte und erörtert mögliche Gegenmaßnahmen.

Keywords: Sicherheit, Bordkarte, Authentifikation

1 Einleitung

PINs und Passwörter sind unsicher, nervig und schwer zu merken. Inzwischen ist fast jedem bewusst, dass man sein Passwort nicht auf einem Post-it an den Bildschirm seines PCs anheften oder auf andere Weise öffentlich zugänglich machen sollte. Dass dies in anderen Situationen immer noch geschieht, zeigen zahlreiche Bilder von Bordkarten auf Facebook oder Instagram. Dass dieses Posting anderen die Möglichkeit gibt, sich auf der Webseite der Fluggesellschaft im Namen des Passagiers einzuloggen, wurde vor kurzem im Blog “Krebs on Security” beschrieben [Kr15]. Ein Leser dieses Blogs konnte nur mit Hilfe eines Bildes der Bordkarte eines Freundes sich bei der Lufthansa einloggen und dort nicht nur den Flug, sondern auch weitere Flüge, die unter seiner Vielfliegernummer gebucht worden sind, einsehen. Desweiteren hätte er auch den Sitzplan ändern oder diesen Flug annullieren können.

Häufig reichen Nachname und Buchungsnummer respektive E-Ticketnummer aus, um bei Fluglinien als auch Touristikunternehmen wie *Checkmytrip* oder *Viewtrip* Flüge zu verwalten. Hat man Zugriff auf das Buchungssystem bekommen, kann man den Sitzplatz wählen oder wechseln, die Bordkarte erneut ausdrucken, Gepäck hinzufügen, den Flug ändern oder sogar annullieren oder eine Bestätigungs-E-Mail erneut senden.

In diesem Artikel untersuchen wir, wie und auf welche Informationen nur durch das Bild einer Bordkarte zugegriffen werden kann und welche Konsequenzen damit verbunden sind – für Sicherheit wie Datenschutz. Wir beleuchten die rechtliche Situation und erörtern technische wie administrative Maßnahmen, um diesen Missbrauch zu erschweren.

¹ Hochschule Luzern – Wirtschaft, Zentralstrasse 9, CH 6002 Luzern, mariia.astrakhantceva@hslu.ch

² Hochschule Luzern – Wirtschaft, Frankenstrasse 9, CH 6002 Luzern, bettina.huebscher@hslu.ch

³ Hochschule Luzern – Wirtschaft, Zentralstrasse 9, CH 6002 Luzern, guenter.karjoth@hslu.ch

2 Der Abflugprozess

Der Ablauf eines Verkehrsflugs von der Buchung bis zum Einsteigen in das Flugzeug ist in Abbildung 1 schematisch dargestellt. Um das stetig ansteigende Personenaufkommen zu bewältigen, hat 2007 die IATA das Simplifying Passenger Travel (SPT) Programm vorgeschlagen [Gu09], dessen Ziel die Optimierung und Automatisierung des Personenverkehrs unter der Berücksichtigung der Sicherheitsvorschriften ist. Es empfiehlt den Einsatz von Self-Service Kiosks, Web Check-in und automatisierten Bordkartenkontrollen.



Abb. 1: Ablauf eines Verkehrsflugs von der Buchung bis zum Einstieg

2.1 Buchung

Um ein Flugticket zu kaufen, wendet man sich entweder an ein Reisebüro, besucht die Webseite der Fluglinie oder einer Buchungsplattform. In einem Online-Buchungsprozess öffnet man zuerst eine Buchungsseite, wählt dort den Flug aus und gibt danach seine Personalien an, welche von Buchungsseite zu Buchungsseite ganz unterschiedlich sein können. Die Website *Seat24*⁴ verlangt Geschlecht, Vor- und Nachname, Email-Adresse und Handynummer. Sobald der Buchungsprozess abgeschlossen ist, speichert das jeweilige Computerreservierungssystem diese Buchung mit einer eindeutigen Kennung – der Buchungs- oder Reservierungsnummer –, und der Nummer des E-Tickets, welche Passagiere per Email (bei einer Online-Buchung) oder in ausgedruckter Form (bei der Reservierung im Reisebüro) bekommen.

Computerreservierungssysteme verwalten Informationen über Fluglinien, Flugpläne, Verfügbarkeit und Tarife. Sie ermöglichen Reservierungen und unterstützen die Ticketausstellung. Weltweit haben sich vier Systeme etabliert: Amadeus, Galileo, Sabre und Worldspan. Jährlich werden mehr als 400 Millionen Tickets bearbeitet. Die Buchungsnummer kann man sich als einen Schlüssel zur Verwaltung einer Buchung vorstellen. Diese Nummer besteht immer aus einer Kombination von sechs Zahlen und Großbuchstaben, z.B. AHY6H0. Es ist wichtig zu wissen, dass der Buchungscode zur Buchung und nicht zum Flug gehört. D.h., wenn innerhalb einer Buchung 10 Flugtickets für fünf Personen gekauft werden, wird nur ein Buchungscode erstellt, mit dem man die ganze Buchung verwalten kann. Die Nummer des E-Tickets ist im Vergleich zum Buchungscode länger und besteht aus 13 Zahlen. Die ersten drei Zahlen sind der IATA-Prefixcode der jeweiligen Fluglinie. Danach folgt die vier-stellige Ticketnummer und die sechs-stellige Seriennummer.

⁴ www.seat24.de

2.2 Check-in

Bei vielen Fluglinien können Fluggäste den Check-in auf deren Website selber durchführen (*Web Check-in* oder *Mobile Check-in*) und dabei auch Sitzplätze und Speisen auswählen. Sie erhalten – papierlos – eine Bordkarte, die mit einem Barcode versehen ist, mittels elektronischer Kurzmitteilung oder Email zugeschickt. Bei Bedarf kann diese auch auf dem eigenen Drucker – zu Hause wie im Hotel – ausdruckt werden (Homeprint). Dieser Dienst wird sehr gut angenommen, obwohl Kosten beim Konsumenten anfallen (Smartphone, Drucker, usw.). Die Fluggäste ersparen sich im Gegenzug einen Teil der Wartezeit am Flughafen [Lu15, S. 61f]. Die Gepäckabgabe erfolgt anschliessend am “Bag-Drop” Schalter im Flughafen. Kunden ohne Internetzugang checken sich am Check-in-Schalter oder an einem Automaten ein [FI15].

Sollte der Akku des Mobiltelefons leer sein, oder man hat sein Mobiltelefon vergessen, so kann man sich jederzeit an einem Check-in-Automaten, am Gepäckabgabeschalter oder am Check-in-Schalter am Flughafen eine Papierbordkarte ausdrucken (lassen).

2.3 Zugang zum kontrollierten Bereich des Flughafen

Flughäfen sind in verschiedene Sicherheitsbereiche unterteilt, deren Zutritt unterschiedlich kontrolliert wird. Der Besitz einer gültigen Bordkarte gibt Zugang zum kontrollierten Bereich des Flughafen. Die Bordkartenkontrolle werden durch automatische Anlagen durchgeführt, die aus einer Sensorschleuse mit automatischen Schwenkflügeln bestehen. Ein integrierter Bordkartenleser erfasst Barcodes von der Bordkarte, dem Homeprint oder auch dem Handy. Die Sensorik sorgt für Einzelzugang der Passagiere. Bei der darauffolgenden Sicherheitskontrolle wird nur die Person und das Gepäck, aber nicht mehr die Bordkarte kontrolliert.

Bei der Verwendung zweier identischer Bordkarten wird der Zugang beim zweiten Versuch gesperrt.⁵ Wenn man vor dem originären Besitzer der Bordkarte den kontrollierten Bereich des Flughafens betritt, ist es damit möglich sich ohne Identitätskontrolle, aber nicht ohne Sicherheitskontrolle, im Flughafen zu bewegen.

3 E-Ticket und Bordkarte

260 oder 83% aller Fluglinien sind Mitglieder des Internationalen Luftverkehrs-Verbandes (IATA). Eine Aufgabe der IATA ist es, die Prozesse im Luftfahrtgeschäft zu vereinfachen. Im Bereich der Fluggastbeförderung betrifft dies auch die Vereinheitlichung der Tickets, so dass der Passagier mit einer einzigen Buchung problemlos mit mehreren Fluglinien reisen kann. Im Rahmen des “Simplifying the Business (StB)” Programm stellten alle IATA Mitglieder bis zum 1. Juni 2008 auf ein elektronisches Ticketsystem um. Neben einer hoher Kostenersparnis (ca. 3 Milliarden \$ pro Jahr), brachte das E-Ticket auch eine Erleichterung für Passagiere bei Ticketverlust oder Änderung ihrer Buchung.

⁵ Gemäß Auskunft vom Flughafen Zürich vom 13. September 2015. Siehe aber Kapitel 5.2.

3.1 Bordkarte

Der obligatorische Text und die Grösse einer Bordkarte sind in der IATA Resolution 722c geregelt [IA15b]. Eine Bordkarte im ABT Format enthält mindestens die folgenden Felder: Fluglinie, Name des Passagiers, Sequenznummer, Abflugort, Ankunftsort, Flugklasse, Tickettyp, Flugnummer, Datum des Flugs, Abflugzeit, Boardingzeit, Sitzplatznummer und das Gate.



Abb. 2: Bordkarte im ABT Format [IA15b]

In der Regel stehen weiter die Nummer des E-Tickets, ein Strichcode/QR-Code und oft der Buchungscode auf der Bordkarte. Diese Daten dienen zur Registrierung und Kontrolle im Flughafensystem des Passagiers vom Check-in bis zum Boarding.



(a) Mobile Bordkarte mit QR-Code [Lu15] (b) Ausgedruckte Bordkarte mit Strichcode [IA15b]

Abb. 3: Elektronisch übermittelte Bordkarten

Neben der am Check-in Schalter erhaltenen Bordkarte (Abbildung 2) sieht man immer öfter mobile Bordkarten auf Smartphones oder Smartwatches (Abbildung 3(a)) oder die zu Hause ausgedruckte Bordkarte (Abbildung 3(b)). Beide Kartentypen enthalten einen

Strichcode oder QR Code. Vor- und Nachteile einer mobilen Bordkarte werden in [Go09, SI15] diskutiert.

3.2 Strichcode und QR-Code

Die im Strichcode gespeicherte Information regelt die IATA Resolution 792 [IA10]. Gemäß dieser Resolution enthält der Strichcode neben der bereits aufgeführten Information noch die Nummer des E-Tickets, den Buchungscode und den Status des Passagiers. Desweiteren sind verschiedene Sicherheitsinformationen enthalten.

Mit der App Barcode Reader pdf417⁶ haben wir den Strichcode zweier uns zur Verfügung stehender Bordkarten ausgelesen. Es zeigte sich, dass die Information im folgenden Format im Strichcode gespeichert ist (zum Datenschutz haben wir Name, Buchungscode und die Vielflieger-Nummer geändert):

M1MUSTERMANN/HANSMR ELKM5HKM HYDBOM9W 452 039H016A0033
10F>10B1WW5039B9W

Diese Information lässt sich leicht in die folgenden Bestandteile auflösen, wie in Tabelle 1 gezeigt. Wenn der Passagier seine Vielfliegernummer der Fluglinie angegeben hat, ist diese Nummer im Strichcode ebenfalls gespeichert.

Information	Beschreibung
M1	leg without conditional data
MUSTERMANN/HANS	Nach- und Vorname des Passagiers
MR	Geschlecht des Passagiers
E	Kennzeichnung E-Ticket
LKM5HK	Buchungscode
HYDBOM	Abflug in Hyderabad (HYD), Ankunft in Mumbai (BOM)
9W 452	Flugnummer
039	Julianisches Datum des Fluges – in diesem Fall der 8. Februar
0033	Sequenznummer des Passagiers – in diesem Fall war der Passagier die 33. Person, welche sich für den Flug eingeecheckt hat
10F>10B1WW5039B9W	spezifische Information für die Fluglinie

Tab. 1: Die im Strichcode gespeicherte Information

Der QR-Code der mobilen Bordkarte enthält noch mehr Informationen als der Strichcode. Um das zu bestätigen, haben wir den gültigen QR-Code einer mobilen Bordkarte von Swiss Airline genommen und mit Hilfe der Internetseite Zxing⁷ dekodiert:

M1MUSTERMANN/HANSMR EAA2BBS ZRHSFOLX 0038 253Y000A0000 03A>10B0 ILX
297421234567891 0LX LX 123456789123456 1PC

⁶ pdf417.mobi

⁷ <https://zxing.org/w/decode.aspx>

Wie man aus der dekodierten Information sehen kann, kommen im QR-Code die Nummer des E-Tickets (7421234567891) und die Vielfliegernummer (123456789123456) hinzu.

4 Angreiferschemen und Konsequenzen

Wie bereits erörtert reichen oft Nachname und Buchungsnummer respektive E-Ticketnummer aus, um bei Fluglinien als auch Touristikunternehmen Flüge verwalten zu können. Bei der Buchung wird diese Information dem Kunden per Email oder Kurznachricht mitgeteilt. Nach dem Check-in ist diese Information auch auf der Bordkarte ersichtlich. Wir stellen uns nun die Frage, wer außerdem Zugriff auf die Bordkarte haben könnte und was mit dieser Information möglich ist.

Bei der Papierbordkarte haben neben dem Passagier häufig Personen aus dem Freundes- und Bekanntenkreis Gelegenheit diese Daten einzusehen. Weitere Personen sind das Reinigungspersonal des Flughafens oder Hotels, welche weggeworfene Bordkarten oder deren Coupons entsorgen. Außerdem bieten viele Hotels die Möglichkeit an, die Bordkarte auf dedizierten und häufig auch für andere leicht zugänglichen Druckern auszudrucken. Mit Angabe der Information übernimmt sogar die Hotelrezeption das Einchecken.

Ein Bild der Bordkarte wird ebenfalls wie beobachtet mit Freunden in sozialen Netzwerken geteilt. Begrenzen die Datenschutzeinstellungen nicht die Sichtbarkeit des Postings, kann auch jeder andere Internetnutzer diese Posts ansehen. Sind Name und E-Ticket Nummer/Buchungscode nicht verdeckt, können diese ohne weitere Hilfsmittel abgelesen werden. Ansonsten reicht es aus den Barcode auf dem Foto zu scannen, um an obige Information zu kommen. Auch wenn auf dem Foto der Barcode nicht gut abgebildet ist, ist die Software der Barcode Scanner häufig in der Lage die Kodierung zu rekonstruieren.

Schlussendlich ist es ebenfalls leicht möglich durch den Kauf eines (billigen) Fluges über das Internet in den Besitz einer Bordkarte zu kommen. Die Identität des Käufers wird dort auf das verwendete Zahlungsmedium reduziert. Wir gehen aber davon aus, dass beim Durchschreiten der automatisierten Kontrolle am Übergang vom öffentlichen in den nicht öffentlichen Bereich eine Videoaufnahme gemacht wird. Bei beiden Arten des Zugangs gilt aber:

“Wer einen Flugschein erwirbt oder sonstwie in den Besitz eines solchen gelangt ohne die Absicht, die Flugreise auszuführen, ist zum Zutritt mittels dieses Flugscheins nicht berechtigt.” [Z14, Art. 3]

Als Berechtigung gelten für Fluggäste die zum Durchschreiten der Zutrittskontrolle und der Passkontrolle notwendigen Ausweise. Diese Ausweise sind nur gültig für den Weg zum und vom Luftfahrzeug.

4.1 Experimente

Wir haben Fotos mit Bordkarten von der Internetseite *WEBSTA*⁸ entnommen. Auf vielen war es leicht den Namen des Passagiers, die Nummer des E-Tickets, die Fluglinie und den Buchungscode zu erkennen. Auf vielen dieser Fotos war auch der Strichcode sichtbar. Diese Strichcodes wurden mit der App Pdf417 und der Internetseite Zxing dekodiert. Die ausgelesenen Daten ermöglichten den Zugriff auf die Buchungsverwaltung.

Am Flughafen Zürich stellten wir fest, dass zum Inhalt der Mülleimer nur das Reinigungspersonal Zugriff hat. Aber es ist anzumerken, dass viele Passagiere vor dem Abflug einfach ihre Bordkarte auf dem Tisch im Café liegen lassen. In der Nähe sitzende Personen könnten daher leicht ein Foto der Bordkarte machen oder den Barcode einscannen.

Außerdem wurde im September 2015 ein Flug von der Schweiz nach Dänemark gebucht, den Web Check-in gemacht und geschaut, wie weit man im Flughafen nur mit einer zu Hause ausgedruckten Bordkarte (ohne Kofferabgabe) gehen kann, ohne dass der Ausweis des Passagiers kontrolliert wird. Während des Abflugprozesses wurde die Bordkarte niemals mit dem Ausweis des Passagiers verglichen. Dies bekräftigt, dass auf Reisen im Schengen-Raum Passagiere selten auf ihre Identität geprüft werden.⁹

4.2 Statistik

Um einen Anhaltspunkt zu bekommen, wie viele Bordkarten im Internet veröffentlicht werden, haben wir über einen Monat nach dem Hashtag #boardingpass in *WEBSTA* gesucht. Auf dieser Webseite wurden pro Tag zwischen 50 und 60 mal das Foto einer Bordkarte veröffentlicht, manchmal waren es sogar 100 Postings. In Stichproben verwendeten wir Bordkarten von verschiedenen Fluglinien, um Zugriff auf die Buchungsinformation zu gelangen.

Obwohl die Klassifizierung von Bildern im Allgemeinen als schweres Problem gilt, haben Lorenzi und Vaidya gezeigt, dass es relativ einfach ist Dokumente wie Kreditkarten, Führerscheine und Pässe im Internet zu finden [LV11]. Bilder mit diesen Gegenständen können mit einer hohen Sicherheit (größer 90 %) erkannt werden. Wir gehen davon aus, dass Bordkarten auf Grund ihrer einfachen Form und vorgegebenen Informationsfeldern ebenso leicht zu erkennen sind. Damit wäre es möglich, auch andere Informationsquellen als *WEBSTA* zu durchforsten.

Wir überprüften die Webseiten von 246 IATA Fluglinien auf die verwendeten Einlogprozedur für die Online Buchungsverwaltung. Wir stellten fest, dass 19% der Fluglinien keine Online-Buchungsverwaltung anbieten. Die am häufigsten verwendete Authentifikationsmethode (50 %) verlässt sich auf die Nennung von Nachname und Buchungscode. Danach

⁸ websta.me

⁹ Die Reise wurde vor den Terroranschlägen am 13. November 2015 in Paris unternommen. Am Flughafen EuroAirport in Basel müssen seit dem bis auf weiteres alle Passagiere einen Ausweis beziehungsweise einen Pass beim Einsteige-Gate vorzeigen, bevor sie das Flugzeug betreten.

kommt Name mit Buchungscode oder Name mit Nummer des E-Tickets (26%). Somit kann man bei Dreiviertel aller untersuchten Fluglinien (76%) sich mit Hilfe von der Bordkarte ablesbarer Information einloggen. Nur 5% aller Airlines verwenden eine Einlogprozedur, welche einen weiteren Eingabeparameter benötigt, wie z.B. die Email-Adresse.

5 Mögliche Schäden und Abwehrmaßnahmen

Wird die Buchungsinformation missbräuchlich verwendet, können Schäden sowohl für den Passagier als auch für die Fluglinie und den Flughafen entstehen. Der Passagier erleidet einen Verlust der Privatsphäre,¹⁰ hat möglicherweise zusätzliche Kosten im Falle der Stornierung des Fluges und verliert Zeit bei einer Nachkontrolle. Die Risiken für die Fluglinie beinhalten eine Rufschädigung und Schadenersatzforderungen. Da der kontrollierte Bereich des Flughafens ohne Antritt des Fluges wieder verlassen werden kann, ist ein Einkaufen im Duty Free Shop möglich.

Wie gut ist ein Passagier im Fall eines Missbrauchs rechtlich geschützt? Jede Fluglinie listet auf ihrer Webpräsenz die Rechte und Pflichten sowohl des Passagiers als auch der Fluglinie. Grundsätzlich sollte jeder Passagier diese Bedingungen lesen, um seine Rechte und die Rechte der Fluglinie zu wissen. Wir haben uns die Beförderungsbestimmungen einiger Fluglinien angeschaut. Auf den Webseiten der Lufthansa fanden wir nur diesen Satz, der die Fluggäste über einen sorgfältigen Umgang mit der Bordkarte informiert:

“Flugscheine sind wertvoll. Sie sind zur sorgfältigen Aufbewahrung und zur Ergreifung der erforderlichen Vorkehrungen gegen Verlust und Diebstahl verpflichtet.”
[LH14, §3.1.8]

Mit dem Posten eines Fotos der Bordkarte ist diese weder gestohlen noch verloren gegangen. Was gilt, wenn Dritte die Information von der Bordkarte ablesen und missbrauchen?

5.1 Luftbeförderungsvertrag

Durch die Online-Buchung eines Flugtickets, wo die entsprechenden Bedingungen (AGB und weitere Vertragsbestandteile) durch Anklicken eines entsprechenden Buttons Gültigkeit erlangen, ist ein Vertragsverhältnis zwischen dem Flugpassagier und der Fluggesellschaft entstanden. Einzige Schranken bilden das Montrealer Übereinkommen [ICAO], gemäß dem der Luftfrachtführer u.a. für Schäden durch Annullierung einer Personenbeförderung haftet.

In ihren Allgemeinen Beförderungsbedingungen (ABB) weist die Lufthansa darauf hin, dass der Fluggast nur mit Vorweisen eines Flugscheins bzw. elektronischer Buchung an

¹⁰ In einem Fall konnten wir mit Hilfe der Buchungsnummer die komplette Europareise einer arabischen Familie einsehen.

der Beförderungsleistung berechtigt ist. Es wird ausdrücklich festgehalten, dass der Flugschein nicht übertragbar ist. Der Fluggast hat die Pflicht, den Flugschein sorgfältig aufzubewahren und darüber hinaus die erforderlichen Vorkehrungen gegen Verlust und Diebstahl zu treffen. Wenn dies auch auf den Schutz vor Missbrauch zutrifft, stellt sich die Frage „Mit was muss der Konsument rechnen?“ Wenn Verlust und Diebstahl genannt ist, wird wohl auf die physische Entwendung des Tickets hingewiesen und wohl kaum auf die Möglichkeit durch den Erhalt von Angaben auf dem Ticket einen Flug zu stornieren oder oder gar selber in Anspruch zu nehmen.

Kann ein Mitwirken des Fluggastes, aber auch durch Dritte, in Bezug auf einen allfällig entstandenen Schaden bejaht werden, so wird die Haftung seitens der Lufthansa entweder ausgeschlossen oder gemindert. Gilt nun das ins Netz gestellte Foto mit dem Ticket als Mitverschulden oder wäre hier nicht mehr die Pflicht beim Dienstleister, die Kunden auf diesen möglichen Missbrauch hinzuweisen? Die Klärung des Umfangs der Informationspflicht und die Überwälzung der Haftung durch die ABB auf den Kunden ist nicht die einzig zu klärende Frage.

Ebenfalls ist auch der Datenschutz mit seinen Vorschriften zu beachten und es ist zu prüfen, ob diese beim genannten Vorfall eingehalten werden. Einer der wichtigsten Grundsätze für die Bearbeitung von Personendaten ist derjenige der Datensicherheit, die fordert, dass Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden. Damit soll verhindert werden, dass die Personendaten durch (externe) Dritte missbraucht werden können, was im vorliegenden Fall sicherlich nicht erreicht wird. Durch Firewalls kann verhindert werden, dass von außen ungehindert auf Informationssysteme zugegriffen werden kann. Wir setzen dies gleich, dass das Flugunternehmen hier eine sichere Variante des Loginsystems anbieten muss, um einen Datenmissbrauch durch Dritte zu verhindern.

Keine Rolle hierbei spielt, auf welche Art und Weise die Schutzziele bedroht sind. Das kann sich aus einem Fehlverhalten eines Mitarbeiters oder eben wie vorliegend aus einem Hacking-Angriff von Dritten ergeben. Aufgrund der Einfachheit des Systems ist ja gar kein Hacking-Angriff als solcher notwendig. Gemäss der Datenschutzverordnung¹¹ müssen die organisatorischen und technischen Massnahmen dazu führen, dass Risiken, d.h. Datenschutzverletzungen verhindert werden. Dazu gehört, dass das Unternehmen eine Risikoanalyse (z.B. Risiko einer unbeabsichtigten/unberechtigten Datenweitergabe, -löschung oder -bearbeitung, eines Datenverlustes oder technischen Fehlers, etc.) durchführt und entsprechende Massnahmen in die Wege leitet. Stellt das Unternehmen im Rahmen seiner Abklärungen fest, dass Vorschriften verletzt werden, muss sie Korrekturmassnahmen empfehlen können. Das heisst also, dass die zu erfassende Risikoanalyse durch den Flugbetreiber eben solche möglichen Gefährdungen aufzeigen soll und Massnahmen daraus abgeleitet und umgesetzt werden.

¹¹ SR 235.11, Verordnung zum Bundesgesetz über den Datenschutz, www.admin.ch

5.2 Gegenmaßnahmen

Da die rechtliche Verantwortung nicht vollständig geklärt ist, sollten die Fluggäste ihre Bordkarten sorgfältig aufbewahren und insbesondere keine Fotos davon im Web veröffentlichen, gebrauchte Bordkarten oder deren Coupons sicher entsorgen und im Flughafen Bordkarten nicht sichtbar in der Tasche oder Portmonee tragen. Ebenfalls ist es notwendig darauf hinzuweisen, dass Barcodes leicht ausgelesen werden können.

Für Fluglinien wie Flughafenbetreiber ist es wichtig, dass die Passagiere im Rahmen der Flugbuchung ausreichend über die Gefahren informiert werden, die durch eine Veröffentlichung einer Fotografie der Bordkarte im Internet bestehen. Diese Maßnahme ist kostengünstig und kann schnell eingeführt werden, da die bestehende Infrastruktur beim Abflugprozess unverändert bleibt. Wie dies gemacht werden kann, zeigt eine aktuelle Meldung der Schweizer Koordinationsstelle zur Bekämpfung der Internetkriminalität KOBIC, in der sie davor warnt, Fotos von Dokumenten mit persönlichen Daten Dritter im Internet zu veröffentlichen, da diese missbraucht werden können [Ko15].

Eine reaktive Maßnahme ist die Speicherung der IP-Adresse, von der eine Buchungsänderung vorgenommen wird. Es erleichtert die Angreifersuche im Falle eines Mißbrauchs. Die Idee ist nicht neu. Die Fluglinie Lufthansa speichert IP-Adressen, wie Malte Spitz in seinem Buch [Sp14] bestätigt. IP-Adressen und Cookies werden von vielen Webseitenbetreibern gespeichert, wie auch Viewtrip und Checkmytrip in ihren Datenschutzbedingungen erläutern. Jedoch ist es möglich die IP-Adresse zu verschleiern.

Eine aktive Maßnahme ist die Überwachung der Doppelverwendung einer Bordkarte beim Zutritt zum kontrollierten Bereich des Flughafens, wie bereits in Kapitel 4 beschrieben. Obwohl technisch einfach zu verwirklichen und auch vom Flughafen bestätigt, scheint hier die Tücke im Detail zu bestehen. Im Januar 2016 ist es am Flughafen Zürich einem Paar mit Hilfe der ausgedruckten Bordkarte und der mobilen Bordkarte gelungen gemeinsam mit nur einem Ticket bis an das Gate zu kommen [20min]. Gemäß Auskunft Flughafen lag es an den Barcodes der Fluglinie Air France, da diese bei mobiler und ausgedruckter Bordkarte nicht identisch waren.

Die heute gebräuchliche Einlogprozedur für die Buchungsverwaltung verhindert wie aufgezeigt den Mißbrauch nicht, da sie sich auf Information stützt, die als geheim betrachtet wird – Name und Buchungsnummer/E-Ticketnummer. Es sollte daher eine zusätzliche Information, die nicht auf der Bordkarte vermerkt ist, zur Authentifizierung mitverwendet werden. Diese Maßnahme ist bereits bei einigen Fluglinien wie Easyjet implementiert. Neben der Email-Adresse sind weitere mögliche Eingabeparameter die Nummer der Karte, mit der der Flug bezahlt wurde, oder ein Geheimwort. Eine 2-Faktor-Authentifikation, wie heutzutage im Homebanking allgemein üblich, kann durch die Bindung der Bordkarte an ein Mobiltelefon erreicht werden. Zumindest beim Zutritt zum kontrollierten Bereich des Flughafens wäre genug Zeit, um auf einen durch eine SMS übertragenen PIN warten zu können. Ein Mißbrauch durch den Besitzer der Bordkarte ist zumindest erschwert, da die beteiligten Personen sich vor und hinter der Kontrolle befinden und den PIN erst übermitteln müssten.

Seit mehreren Jahren wird auch an die Verwendung von biometrischer Information gedacht [Pr09]. Führt SAS bereits im Jahr 2008 als erste Fluglinie einen optionalen biometrischen Check-in für Inlandflüge ein [GW09], hat sich dieser Ansatz noch nicht durchgesetzt, da es immer noch Pilotprojekte wie von der Alaska Airlines gibt, in denen untersucht wird, inwieweit ein Fingerabdruck die klassische Bordkarte ersetzen kann [Ai15].

Wird der Buchungscode nicht oder nur teilweise auf der Bordkarte aufgeführt, besteht keine Möglichkeit mehr die Originalität der Bordkarte automatisch zu erkennen. Es besteht aber die Möglichkeit die im Barcode kodierte Information zu verschlüsseln [KK14], was aber dessen Kapazität verringert und eine Anpassung der Lesegeräte erfordert. Ausserdem ist die sichere Verwaltung der notwendigen Schlüssel eine große Herausforderung.

6 Fazit

Buchungsinformationen eines Passagiers sind von Dritten einsehbar und können mißbraucht werden, wenn Fotos von Bordkarten auf dem Internet veröffentlicht oder anderweitig zugreifbar sind. Dies kann sowohl Fluggast wie auch Fluglinie schädigen. Name und Buchungsnummer, die zur Authentifikation meistens verwendet wird, ist nicht nur im Klartext auf der Bordkarte abgedruckt, sondern auch in dem Barcode enthalten. Die dadurch entstehende Gefahr ist vielen Passagieren nicht bewußt. Der Einsatz automatischer Bilderkennungsrouitinen erhöht die Gefahr, dass für einen spezifischen Missbrauch die dafür geeignete Bordkarte gefunden werden kann.

Um diese Risiken zu vermindern, gilt es neben einer Aufklärung der Passagiere auch die heute übliche Authentifikation um eine zusätzliche Information, die nicht auf der Bordkarte abgebildet ist, zu erweitern. Ein Verzicht des Aufdruckes von Name und E-Ticketnummer würde wohl die Funktionalität bestehender Systeme beeinträchtigen. Der Einsatz biometrischer Information wäre ein starker Eingriff in die informationelle Selbstbestimmung der Passagiere. Auf jeden Fall gilt es eine transparente Sicherheitsanalyse durchzuführen und sich nicht hinter (geheimen) behördlichen Anforderungen zu verschansen. Die Annahme, dass die Nummer des E-Tickets als ein geheimes Passwort geeignet ist, hat sich als Fehleinschätzung herausgestellt.

Danksagung

Die Autoren danken Konrad Marfurt und den Gutachtern für ihre hilfreichen Kommentare.

Literaturverzeichnis

- [20min] Flughafen Zürich: «Wir konnten mit einem Ticket zu zweit ans Gate» 28. Januar 2016 05:51; Akt: 28.01.2016 09:56, www.20min.ch/schweiz/zuerich/story/-Wir-konnten-mit-einem-Ticket-zu-zweit-ans-Gate-16718494.
- [Ai15] Fingerabdruck statt Bordkarte: Alaska Airlines prüft neue Technik, www.airliners.de/fingerabdruck-bordkarte-alaska-airlines-technik/36405.

- [LH14] Lufthansa: Allgemeine Geschäftsbedingungen – Beförderungsbedingungen für Fluggäste und Gepäck (ABB Flugpassage), www.lufthansa.com/online/portal/lh/cmn/generalinfo?nodeid=1761532.
- [Fl15] Check-in Methoden, www.flughafen-zuerich.ch/passagiere-und-besucher/abflug-ankunft/check-in-methoden.
- [GW09] Glambedakis, A., Watson, G.: Pervasive computers in aviation passenger risk profiling. In *Risk Assessment and Management in Pervasive Computing : Operational, Legal, Ethical, and Financial Perspectives*, pp. 246–261, 2009.
- [Go09] Flugticket fürs Mobiltelefon: schneller, besser, sicherer?, www.zdnet.de/41002453/flugticket-fuers-mobiltelefon-schneller-besser-sicherer/4.
- [Gu09] Gupta, A., Davidson R.: Simplifying passenger travel (SPT) program. In: Third symposium and Exhibition on ICAO MRTDs, Biometrics and Security Standards. 2009.
- [IA10] Passenger Services Conference Resolutions Manual, www.iata.org/whatwedo/stb/documents/resolution792-june2010.pdf.
- [IA15b] Simplifying the Business: Bar Coded Boarding Pass Implementation Guide, www.iata.org/whatwedo/stb/documents/bcbp_implementation_guidev4_jun2009.pdf.
- [Ko15] Koordinationsstelle zur Bekämpfung der Internetkriminalität, KOBIK: Achtung! Veröffentlichen Sie im Internet keine Fotos von Dokumenten, die persönliche Daten Dritter enthalten. <https://www.cybercrime.admin.ch/kobik/de/home/warnmeldungen/2015/2015-09-22.html>, September 2015.
- [ICAO] ICAO: Übereinkommen zur Vereinheitlichung bestimmter Vorschriften über die Beförderung im internationalen Luftverkehr (kurz: Montrealer Übereinkommen), 1999. <https://www.admin.ch/opc/de/official-compilation/2005/4395.pdf>
- [KK14] Krombholz, K.; Frühwirt, P.; Kieseberg, P.; Kapsalis, I.; Huber, M.; Weippl, E.: QR Code Security: A Survey of Attacks and Challenges for Usable Security. *Human Aspects of Information Security, Privacy, and Trust*. pp. 79–90, 2014.
- [Kr15] Krebs, B.: What is in a Boarding Pass Barcode? A Lot. Krebs on Security, 2015. krebsonsecurity.com/2015/10/whats-in-a-boarding-pass-barcode-a-lot.
- [Lu15] Die Mobile Bordkarte - mobil einchecken und Zeit sparen, www.lufthansa.com/ch/de/Die-Mobile-Bordkarte-auf-vielen-Strecken-weltweit-verfuegbar.
- [LV11] Lorenzi, D.; Vaidya, J.: Identifying a Critical Threat to Privacy Through Automatic Image Classification. In: First ACM Conference on Data and Application Security and Privacy (CODASPY '11). ACM, pp. 157–168, 2011.
- [Pr09] Pravir K. Chawdhry, Rui Pareira Da Silva: Advanced registered traveler paradigm using dynamic risk profile and multimodal biometrics. In: *Systems, Man and Cybernetics*. pp. 3946–3951, 2009.
- [SI15] Mobile evolution, www.sita.aero/resources/air-transport-it-review/air-transport-it-review—issue-3-2014/mobile-evolution—beacons-biometrics-wearables.
- [Sp14] Spitz, M.: Was macht ihr mit meinen Daten? Hoffmann und Campe, 2014.
- [Z14] Flughafen Zürich: Betriebsreglement für den Flughafen Zürich vom 30.6.2011, Anhang 3: Zutrittsordnung für das nichtöffentliche Flughafengebiet. Stand am 1. Juli 2014