SBB Ticketdaten im Netz

Zugriff auf ÖV-Buchungen der letzten Jahre

Abschlussbericht

25. Januar 2022

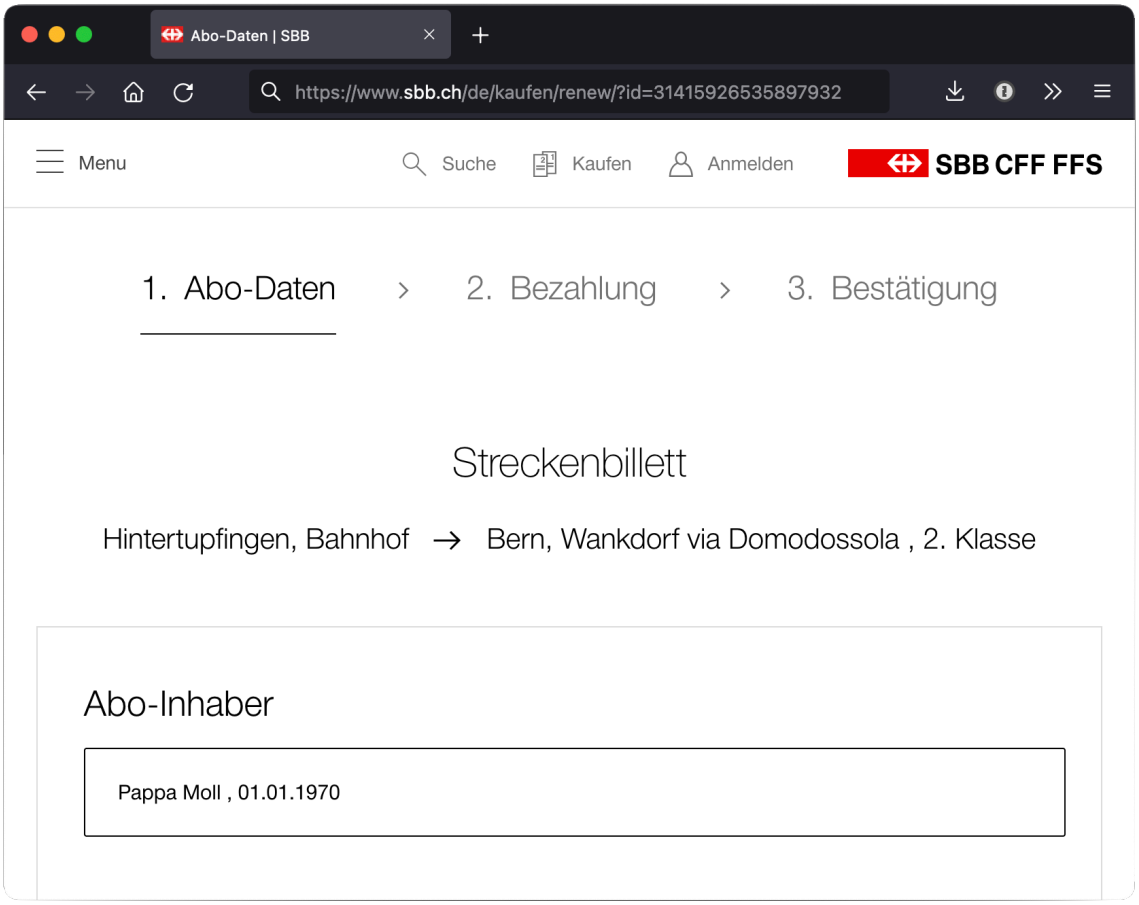
Kontakt über office@digitale-gesellschaft.ch
Publiziert auf https://digitale-gesellschaft.ch/2022/01/27/sbb-sicherheitsluecke

Inhaltsverzeichnis

1 Problem

Ein Verkehrsbetrieb hat ein Remindermail an die Kunden mit dem folgenden Betreff versendet: «Ihr Abo läuft aus - jetzt verlängern.»

Im Mail findet sich ein Link zu einem Webshop, in dem das Abo erneuert werden kann. Der Link lautete: *https://www.sbb.ch/de/kaufen/renew/?id=XXXXXXXXX*



2 Zugriff auf Ticketdaten

Es wurde festgestellt, dass durch Verändern der ID in der oben beschriebenen Inernetseite, auch auf weitere Kundendaten zugegriffen werden kann.

Folgende persönliche Informationen konnten ausgelesen werden:

- Abfahrtsort
- Ankunftsort
- via
- gekaufter Artikel (Streckenbillett, Einzelbilette, Mehrfahrtenkarten etc.)
- Klasse (1. Klasse, 2. Klasse)
- Zonen der lokalen Verkehrsbetriebe
- **Vorname, Nachname**
- **Geburtsdatum (DD.MM.YYYY)**

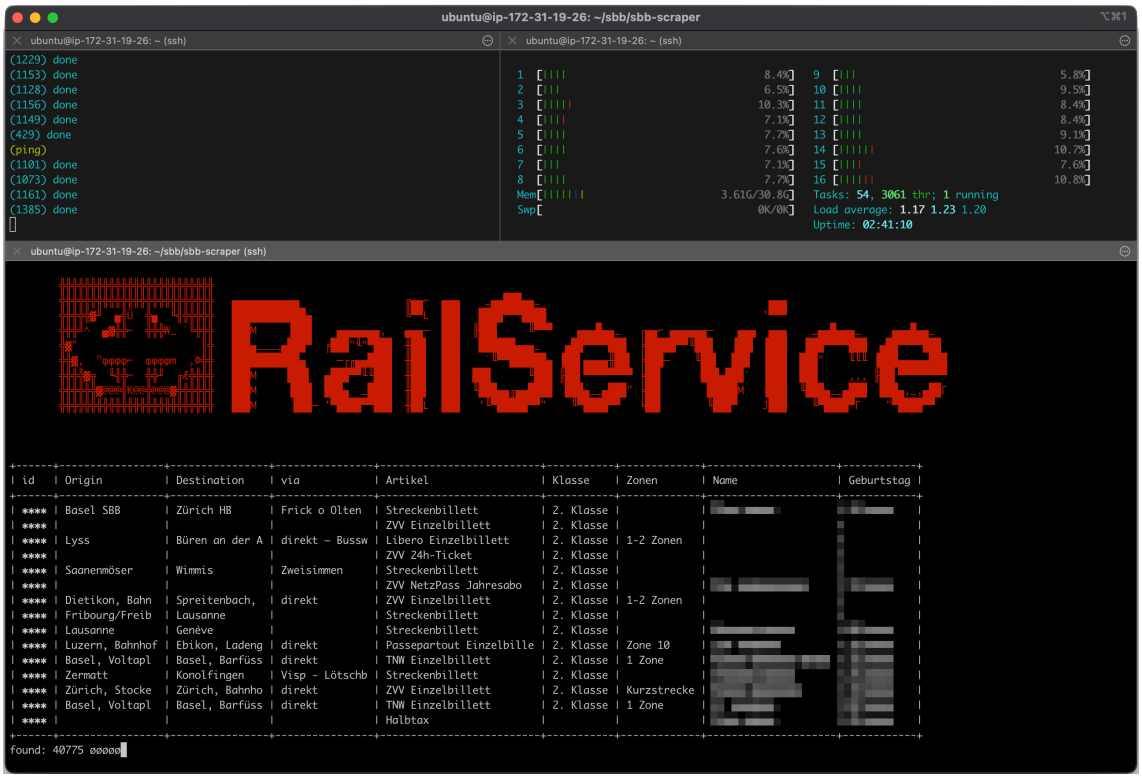
3 Auswirkungen

Durch diese Sicherheitslücke war es möglich, auf sehr viele Ticketbuchungen (mehrere hundert Mio.) zuzugreifen. Betroffen waren sämtliche Ticketbuchungen der zentralen Vertriebsplattform Nova (Netzweite ÖV-Anbindung). Es wurde 1 Mio. Reisebewegungen von 500'000 Reisenden in wenigen Tagen abgegriffen.

Neben den Tickets sind auch Rechnungen (Halbtax-Abo, Monats-GA) zu finden, welche über die zentrale Plattform ausgestellt wurden. Bei weniger als der Hälfte der Funde waren reine SBB-Streckenbillette betoffen. Mehrheitlich stammten die Tickets und Abos von den 250 Unternehmen des Öffentlichen Verkehrs[1].

3.1 Automatisiertes Abfragen

Theoretisch konnten die Daten manuell ausgelesen werden, doch mittels eines kleinen Computerprogramms wurden die Daten um einiges effizienter abgegriffen.



Das Programm lief auf einem Computer mit 16 CPU-Cores und 32GB Memory. So waren 70'000 Abfragen pro Stunde möglich. Wie auf dem Screenshot zu sehen ist, langweilte sich der Computer. Es wurden nur 10% der Maximalleistung verwendet. Aus Rücksicht auf die technische Infrastruktur der SBB wurde nicht aggressiver abgefragt.

Hätte eine angreifende Person ein Interesse gehabt, möglichst viele Daten abzugreifen, wäre das Vorgehen etwas weniger forsch gewesen. Es wäre viel Energie in die Verschleierung der Abfragen gesteckt worden.

Es erscheint unrealistisch, dass der vollständige Datensatz, von der SBB unbemerkt, hätte heruntergeladen werden können. Zumal die Sicherheitslücke nur kurze Zeit ausgenutzt werden konnte.

[1] siehe Alliance SwissPass, https://www.allianceswisspass.ch/de/ueberuns/die-alliance-swisspass

4 Feststellungen

4.1 Lösung: UUID statt ID

Hätte die SBB, die Systembetreiberin der betroffenen Plattform ist, anstatt einer fortlaufenden Zahl einen UUID (Universally Unique Identifier)[2] als Identifikationsmerkmal verwendet, wären die Buchungen nicht so leicht aufzurufen gewesen.

4.2 Unterschiede zwischen den Verkehrsbetrieben

Aufgefallen ist das Problem durch einen Remindermail eines Transportunternehmens. Andere Verkehrsbetriebe verwenden, einen auf den ersten Blick, sicheren, nicht enumerierbaren Link. Ein Beispiel:

https://www.sbb.ch?p=eyJzIjoieGNMM2QzZHk1elltSXVZMmhjWEZ3dlpHVmNYRiIsInYiOjEsInAiOiJ7XCJ1XCI6MzE0MTU5MjYsXCJ2XCI6MSxcInVybFwiOlwiaHR0cHM6XFxcL1xcXC93d3cuc2JiLmNoXFxcL2RlXFxcL2thdWZlblxcXC9yZW5ldz9pZD1YWFhYWFhcIixcImlkXCI6XCJCUkFWTywgRFUgSEFTVCBFUyBLT05UUk9MTElFUlQsIFdJUiBTT0xMVEVOIE1BTCBFSU4gQklFUiBUUklOS0VOIEdFSEVOXCIsXCJ1cmxfaWRzXCI6W1wieU16YzROek5oWkdJNE5qSVwiXX0ifQ

Diese auffällig lange ID ist nicht zufällig, sie ist in base64[3] codiert. Base64 ist eine der gängigsten Methoden, um strukturierte Inhalte im Internet in codierter Form zu übertragen und hat mit Sicherheit oder Verschlüsselung nichts gemeinsam.

Was wir sehen, wenn die obige Adresse decodiert wird, ist die uns bekannte URL. Folgende Daten werden in dem Link übermittelt:


```
{
  "s": "xcL3d3dy5zYmIuY2hcXFwvZGVcXF",
  "v": 1,
  "p": {
    "u": 31415926,
    "v": 1,
    "url": "https://www.sbb.ch/de/kaufen/renew?id=XXXXXX",
    "id": "SUDVlWjhNIiwidiI6MSwicCI6IntcInVcIjoz",
    "url_ids": ["yMzc4NzNhZGI4NjI"]
  }
}
```


4.3 Persönlichkeitsrechte der Reisenden

In den letzten Jahren hat der Autor Dutzende Fahrten im öffentlichen Verkehr gemacht. Die Tatsache, dass jede Person, welche diesen Link kannte, theoretisch das persönliche Reiseverhalten nachvollziehen konnte, hat ihn beunruhigt.

Ein vollständiger Datensatz hätte in den falschen Händen fatale Auswirkungen gehabt: Wird der Datensatz auf die Reisedaten auf eine Person durchsucht, ergibt sich ein Reisetagebuch. Würde der Datensatz mit Personendaten aus weiteren Datenquellen kombiniert, könnten gezielte Phishingangriffe und Identitätsdiebstahl begünstigt werden.

Die gewonnenen Daten des Autors wurden mit den Logfiles der SBB-Server abgeglichen. Es wurde festgestellt, dass keine weiteren Daten abgeflossen sind. Da der Autor die personenbezogenen Daten gelöscht hat, wurden die Persönlichkeitsrechte der Reisenden gewahrt.

[2] z.B. nach RFC3122 https://datatracker.ietf.org/doc/html/rfc4122
[3] siehe https://de.wikipedia.org/wiki/Base64

5 Responsible Disclosure gegenüber SBB

Die hier beschriebene Sicherheitslücke wurde am 9. Januar 2021 der SBB gemeldet. Ansprechsperson war der Chief Information Security Officer (CISO).

- Die SBB hat die Tragweite des Problems schnell erkannt und mit ensprechender Priorität reagiert. Als Sofortmassnahme wurde der betroffene Zugang deaktiviert. Da das betroffene System von sehr vielen Transportunternehmen genutzt wurde, war die Behebung dieser Sicherheitslücke relativ aufwändig.

- Neben der Behebung der Sicherheitslücke hat die SBB auch einen externen Sicherheitsaudit in Auftrag gegeben um sicherzustellen, dass die Lücke definitiv geschlossen wurde.

- Der Report wurde nicht sofort veröffentlicht, um der SBB genug Zeit für die Behebung des Vorfalls zu geben.

Es wurde der SBB empfohlen,

- **dass der Zugriff auf die betroffene Seite deaktiviert wird und anschliessend einen sichere Zugang zu den betroffenen Services angeboten wird.** Der Zugang zu den betroffenen Diensten wurde sofort eingeschränkt und interne Prozesse eingeleitet, um die Dienstleistung auf eine sichere Art anzubieten.

- **dass der eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) umfassend über die Datenschutzverletzung informiert wird.** Eine Meldung an den EDÖB ist bereits in den Prozessen des SBB-Security-Operation-Center verankert und wäre auch ohne den Hinweis des Autors passiert.

- **dass der Autor regelmässig und proaktiv über den Zwischenstand informiert wird.** Aus Sicht des Meldenden war der Kontakt transparent und der Wille zu einer vollständigen Behebung des Problems jederzeit ersichtlich.

- **dass die Reisenden über die Datenschutzverletzung informiert werden.** Der wohl schwierigste Punkt für eine Firma ist es, in dieser Situation Verantwortung zu übernehmen und öffentlich zu kommunizieren. Die SBB war bereit zu einer aktiven Kommunikation gegenüber den Reisenden und hat eine Medienmitteilung veröffentlicht.

Auch wenn es im ersten Moment unangenehm ist, diesen Fehler öffentlich zu machen, steigt das Ansehen der SBB in den Augen des Autors, weil sie dadurch transparent zu gemachten Fehlern steht. In Anbtracht der vielen beteiligten Transportunternehmen hat die SBB sehr schnell reagiert.

Abschliessend kann festgehalten werden, dass die SBB vorbildlich auf die Meldung reagiert hat und die in Bezug zu diesem Report heruntergeladenen personenbezogenen Daten vollständig vernichtet wurden.

Der Autor dankt

- dem CISO für das Managen des Themas und dem Betriebsteam für die rasche und professionelle Behebung der Schwachstelle.
- dem EDÖB und seinem Team für die datenschutzrechtliche Einordnung.
- der Digtalen Gesellschaft für die Unterstützung
- Ein herzliches Brrrrrra dem Korrigör für die Berichtigung der schlimmsten Fähler.

6 Öffentliche Berichterstattung

6.1 Medienmitteilungen

Medienmitteilung der SBB: https://news.sbb.ch/artikel/109673/datenabfluss-bei-oev-vertriebsplattform-festgestellt-und-unterbunden

Medienmitteilung der Alliance SwissPass: https://www.allianceswisspass.ch/de/asp/News/Newsmeldung?filterCategory=4&newsid=363

6.2 SRF Rundschau

Für eine sorgfältige mediale Aufarbeitung dieses Reports wurde Georg Humbel von der «Rundschau» als Medienpartner gewählt. Der TV-Beitrag wurde in der «Tagesschau», dem «10vor10» gezeigt. Auf der Website des SRF ist ein Online-Artikel erscheinen.

Online Artikel: «Datenleck bei der SBB: Swisspass-Daten offen einsehbar» (verlinkt)

Tagesschau Hauptausgabe:

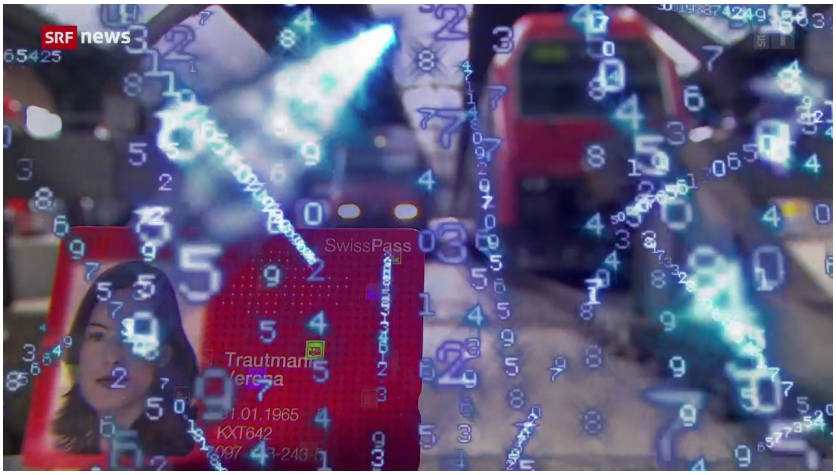


Abb. 1: Tagesschau vom 24.01.2021, ab 0:00 (Video verlinkt)

10vor10:

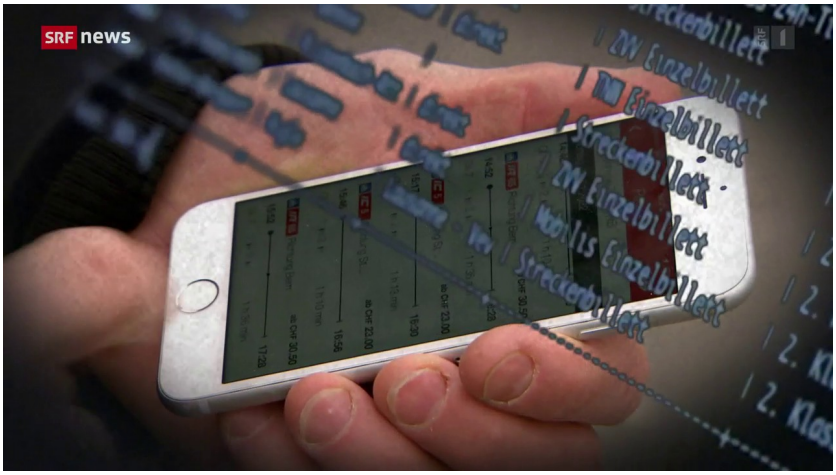


Abb. 2: 10vor10 vom 24.01.2021, ab 7:22 (Video verlinkt)