ALTERNATIVEN

Die IT-Sicherheit von allen drei Anbietern ist auf dem gleichen Level

Booking.com = 

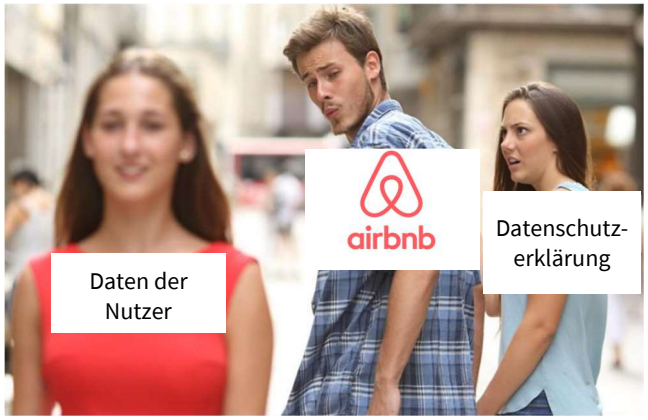
airbnb

EMPFEHLUNGEN

Nach der sicherheitskritischen Analyse von Airbnb mit den aufgedeckten Sicherheitslücken und dem schlechten Umgang mit den Daten der Nutzer können wir aus unserer Sicht nur davon abraten Airbnb zu benutzen. Auch die Analyse der alternativen Internetdienste (Booking.com und FeWo Direkt) führt nicht zu einer Verbesserung der Sicherheit, weshalb wir auch von diesen Internetdiensten abraten. Aufgrund der fehlenden Alternativen mit einem besseren Sicherheitsniveau, muss jeder Benutzer selber entscheiden, ob der Nutzen des Angebotenen Services gegenüber den Sicherheitsrisiken bei einer Verwendung des Dienstes überwiegt.

KURZ UND KNAPP

Airbnb hat die grundsätzlichen IT-Sicherheitsrelevanten technischen Maßnahmen implementiert. Airbnb weißt jedoch grobe Implementierungsfehler auf, die von Angreifern missbraucht werden können, um den Dienst anzugreifen.
Darüber hinaus ist Datenschutz für Airbnb eine Fremdsprache. Daten werden fröhlich von sogenannten „Geschäftspartnern“ gesammelt, untereinander ausgetauscht und anschließend analysiert.



CREDITS:

Andrej Katic, Benedikt Herbst, Kevin Patsch, Niklas Post, Jannis Mücke

Sichere Internet-Dienste
Sommersemester 2019
Prof. Dr. Sachar Paulus

Airbnb & Security

Eine sicherheitskritische Analyse

airbnb

hochschule mannheim

Stakeholder

Mieter

Regierung & Kommunen

Vermieter

Geschäftspartner

Anforderungen

- Sicherer Zugang zum Account
- Sichere Datenspeicherung & Zahlungstransaktionen
- Daten werden Zweckmäßig verwendet
- Profile/Identitäten sind verifiziert/ überprüft
- Schutz der Privatsphäre vor Betrug & Schäden während des Besuchs
- Überprüfung der Unterkünfte auf Richtigkeit aller Angaben

Technische Untersuchung

Sicherheitsrelevante Aspekte wie eine verschlüsselte HTTPS-Verbindung samt gültigen SSL-Zertifikat und einer zwei Faktor Authentifizierung sind vorhanden. Weitere Sicherheitsfunktionen wie Limit Login Attempts zum Schutz vor Brute Force Angriffen, eine automatische Geräteerkennung, um Anmeldungen aus dem Ausland zu verhindern oder die Möglichkeit sich per Single Sign On zu resistieren, sind ebenfalls implementiert.
Potenzielle Sicherheitslücken wurden bei der Absicherung von Cookies, der teilweise unsicheren Implementierung der Content Security Policy, der nicht eingebundenen Subresource Integrity sowie der nicht gesetzten Referrer Policy festgestellt. Hierdurch könnten z.B. Cross-Site Scripting, Data Injection oder Clickjacking Angriffe eine mögliche Bedrohung darstellen.

Positive Sicherheitsaspekte

HTTPS-Verbindung:	+
SSL-Verschlüsselung:	+
Zwei Faktor Authentifizierung:	+
Limit Login Attempts:	+

Potentielle Schwachstellen

Absicherung von Cookies:	-
Content Security Policy:	-
Subresource Integrity:	-
Referrer Policy:	-

Hands-On : Werkzeuge zur Überprüfung von Internetdiensten

Qualys. SSL Labs

Firefox Lightbeam

Observatory moz://a

webbkoll | dataskydd.net