Die Sicherheit von AirBnb

SID, SoSe 2019

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

Agenda

1. **Zum Unternehmen**
   a. Geschäftsmodell im Überblick
   b. USP von AirBnb
   c. Wie funktioniert es?

2. **Stakeholder und deren Anforderungen**
   a. Direkte Stakeholder: Mieter, Vermieter
   b. Indirekte Stakeholder: Regierung, Einheimische

3. **Umsetzung der Anforderungen**
   * AirBnb
   * Vergleich Fewo Direkt
   * Vergleich Booking.com
   * Wissenschaftliche Untersuchung

4. **Architektur der Plattform**

5. **Technische Details der Plattform**

1. Zum Unternehmen

a. Geschäftsmodell im Überblick

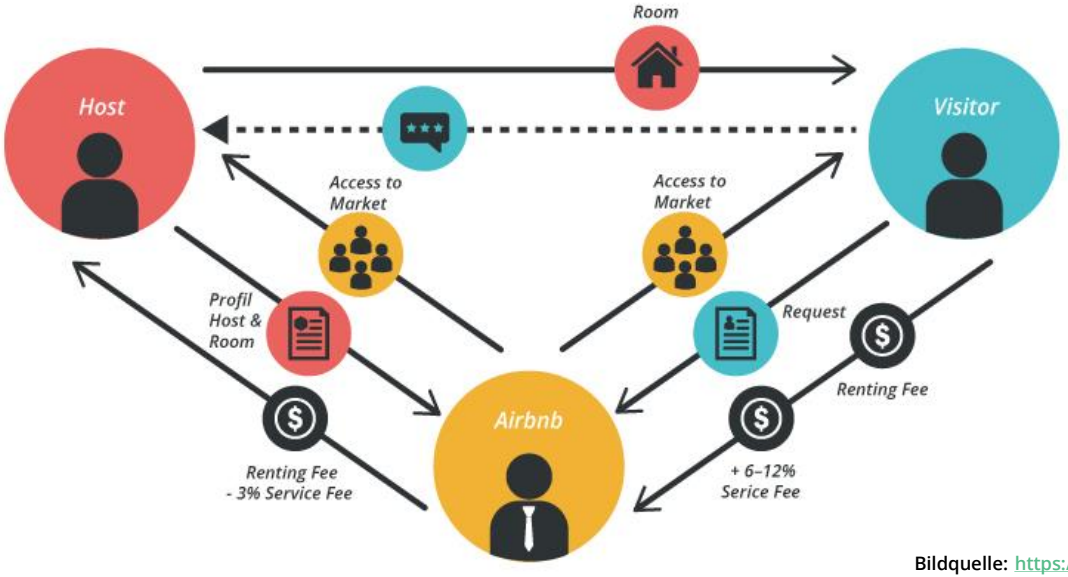
b. USP von AirBnb

c. Wie funktioniert es?

Geschäftsmodell im Überblick

Was ist AirBnb?

- eine Online-Plattform, auf welcher private Unterkünfte vermietet werden



Bildquelle: https://bmtoolbox.net/stories/airbnb/

Geschäftsmodell im Überblick

Was ist AirBnb?

- eine Online-Plattform, auf welcher private Unterkünfte vermietet werden
- weltweit verbreitet: über 5 Millionen Inserate in 191 Ländern
- immer dabei, sein Angebot zu erweitern:
  - Aktivitäten
  - Restaurants
  - neben Privatunterkünften auch Hotelzimmer
  - AirBnb plus

Geschäftsmodell im Überblick

Probleme des Modells

- Beschwerden über kommerzielle und rücksichtslose Nutzer
- Mangel an Wohnraum wird verstärkt
- Vorwurf: illegale Inserate, da keine Steuern gezahlt werden

1. Zum Unternehmen

a. Geschäftsmodell im Überblick

b. USP von AirBnb

c. Wie funktioniert es?

USP von AirBnb

Vergleich mit couchsurfing

- AirBnb richtet sich an diejenigen, die sich üblicherweise in einem Hotel niederlassen würden …

Vergleich mit Booking.com

- … die jedoch eine günstigere Alternative suchen

⇨ AirBnb positioniert sich zwischen Couchsurfing und dem klassischen Hotel

Vergleich mit FeWo-direkt Teil der HomeAway Familie

- AirBnb ist mit seiner Geschäftsidee heute nicht mehr alleine, aber:

→ Qualität der Unterkünfte lässt sich bei AirBnb aufgrund der großen Community besser einschätzen
→ AirBnb als “Lifestyle-Marke”
→ Differenzierung durch Ansprache des Zugehörigkeitsbedürfnisses

Wie funktioniert es?

Glückwunsch! Dein Inserat wurde veröffentlicht! In ein paar Stunden können Gäste dein Inserat finden und buchen, also stelle sicher, dass deine Einstellungen, Preise und Kalender korrekt sind. Schau dir auch dein Dashboard unten an, um Tipps für deine erste Buchung zu erhalten.

Dashboard

Übersicht deiner Inserate

Schöne und ruhige Wohnung in Ludwigshafen
Ludwigshafen am Rhein, Deutschland
Bearbeiten · Wechseln

Tipps, wie du Buchungen erhältst

Du bist auf dem besten Weg. Mit jedem abgeschlossenen Tipp kannst du bis zu 15 % mehr Aufrufe deines Inserats erwarten.

Teste einen niedrigeren Mindestpreis Mach dein Inserat wettbewerbsfähiger, indem du unseren Tipp für den Mindestpreis nutzt.

Aktualisieren

Tipp: Wenn du einen Mindestpreis von 6€ festlegst, hast du

1. Zum Unternehmen

a. Geschäftsmodell im Überblick

b. USP von AirBnb

c. Wie funktioniert es?

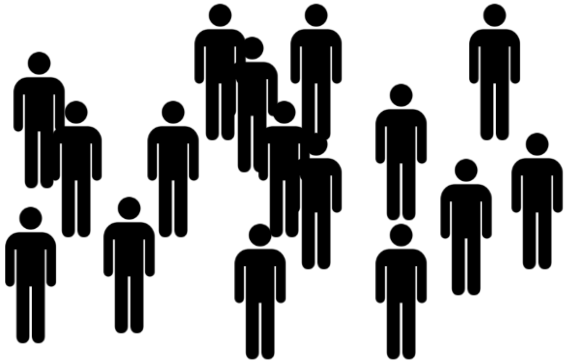
2. Stakeholder und deren Anforderungen

a. Direkte Stakeholder

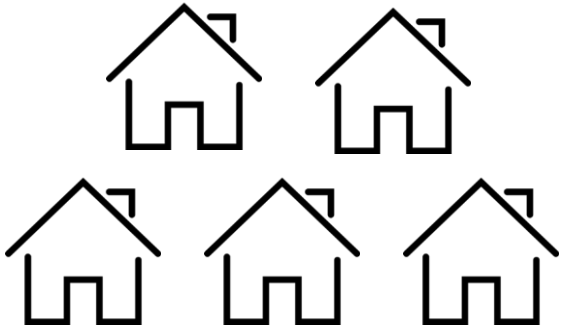
b. Indirekte Stakeholder

Direkte Stakeholder

17 Mio. Gäste



640.000 Vermieter



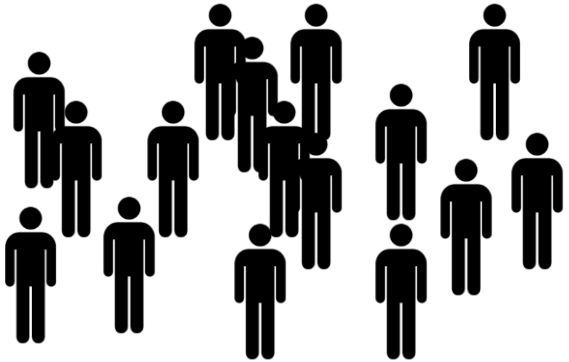
2. Stakeholder und deren Anforderungen

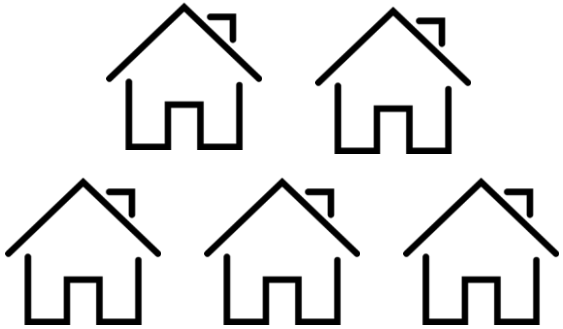
a. Direkte Stakeholder

b. Indirekte Stakeholder

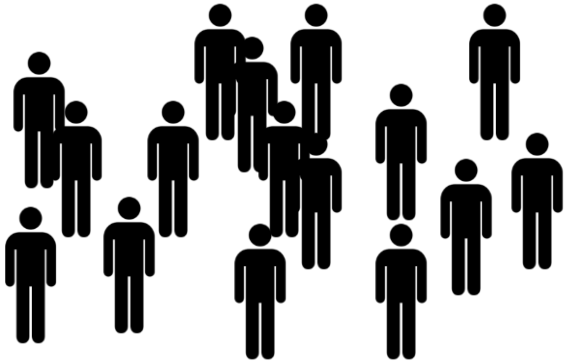
Indirekte Stakeholder

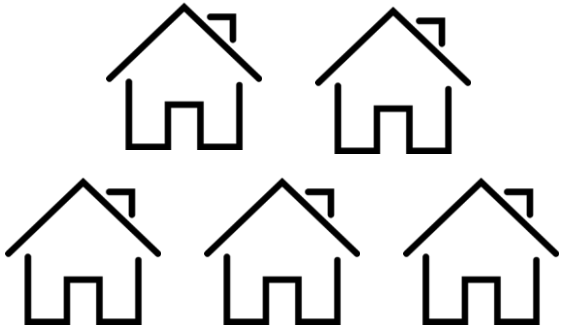
airbnb



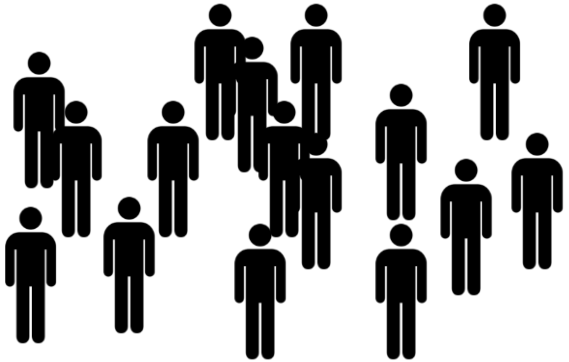


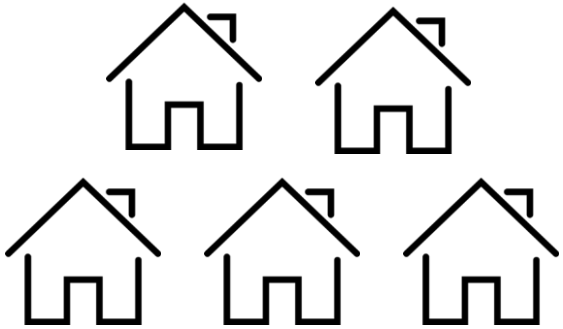
Indirekte Stakeholder





Indirekte Stakeholder



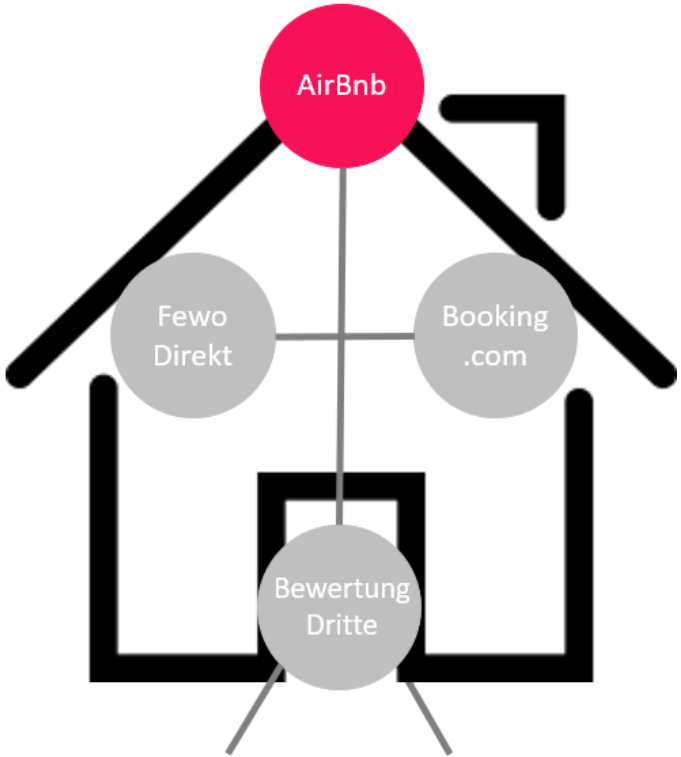


3. Umsetzung der Anforderung

Technische Anforderungen:
Sicherer Zugang zum Account

Stakeholder: Mieter, Vermieter

Sicherer Zugang zum Account



- ➔ Erstelle ein eindeutiges Passwort
- ➔ Mindestens acht Zeichen und häufig genutzte Kombinationen vermeiden
- ➔ Hol dir einen Passwort-Manager

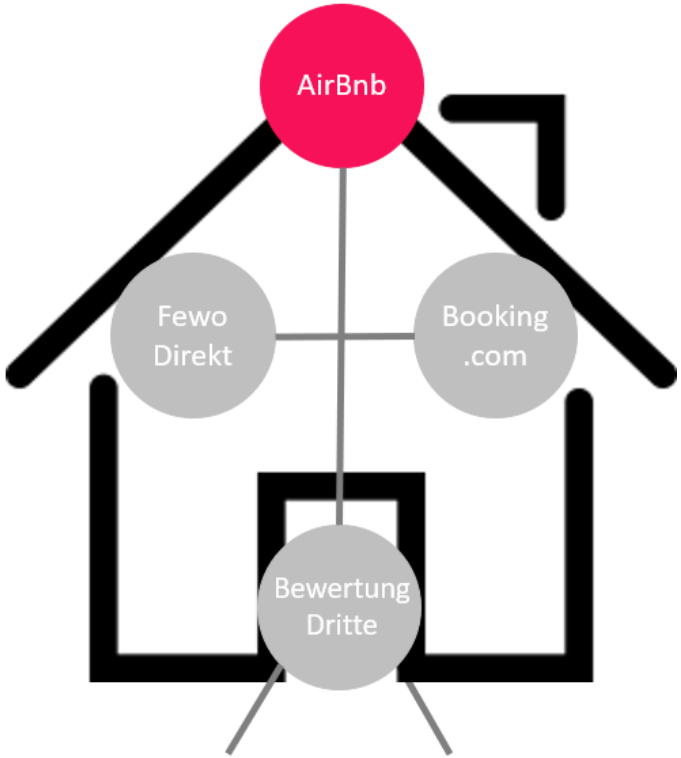
Häufigste Sicherheitslücke

- ➔ Jemand erhält über ein herausgefundes Passwort Zugang zu einem Account

Was gefährdet das Passwort?

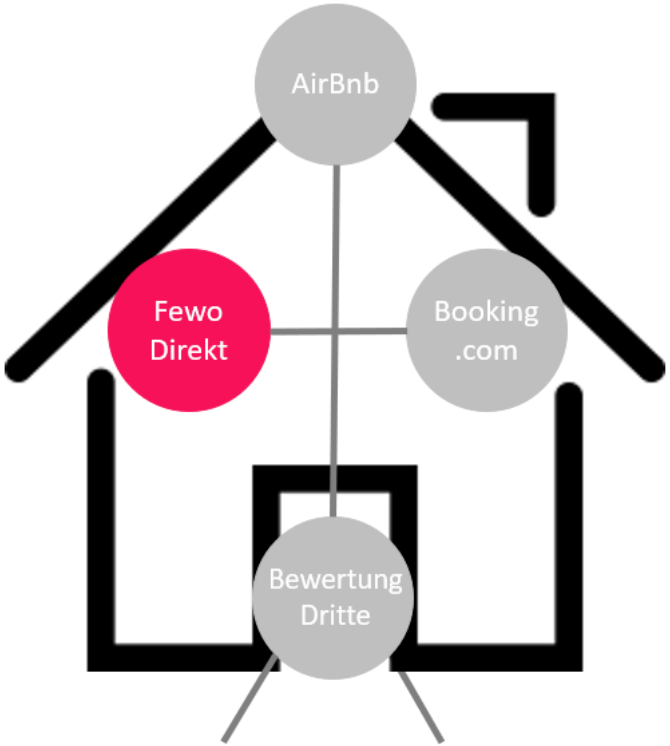
- ➔ Passwort Listen im Internet
- ➔ Phishing
- ➔ Malware

Sicherer Zugang zum Account



- ➔ Maschinelle Lerntechniken
- ➔ Multi-Faktor Authentifizierung
- ➔ Kontowarnungen

Sicherer Zugang zum Account

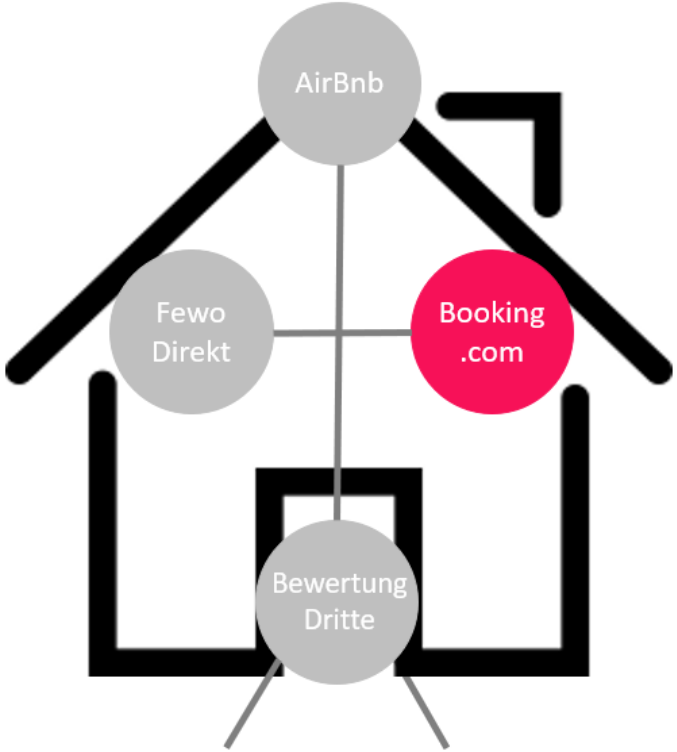


- ➔ Sensibilisierung
- ➔ Passwortrichtlinien Schwach
- ➔ 2 Faktor Authentifizierung

FeWo-direkt
Teil der HomeAway Familie

~

Sicherer Zugang zum Account



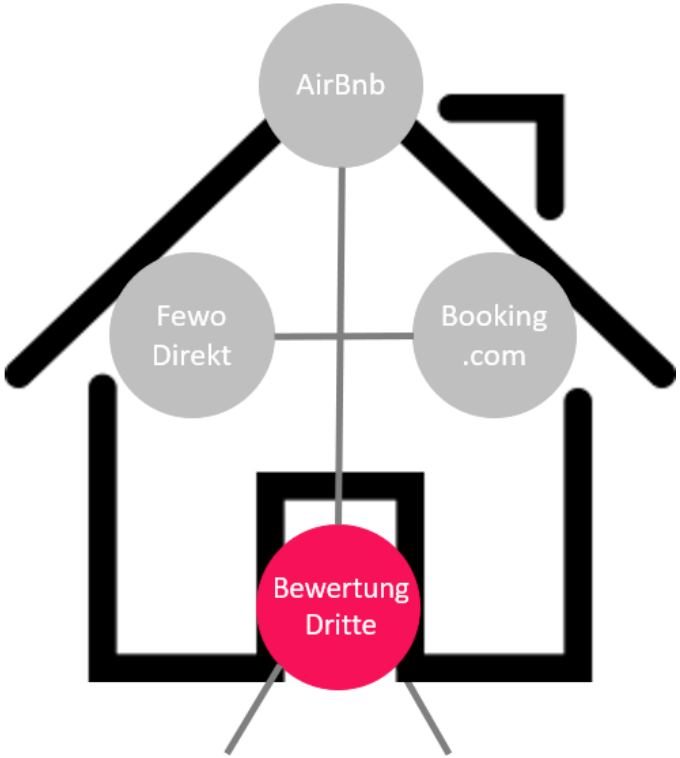
➔ Persönliche Daten werden für Gefährdungs-beurteilungen und Sicherheitszwecke, einschließlich der Authentifizierung der Nutzer genutzt

Bewusstsein für Online Sicherheit

➔ Social Engineering

➔ 2-Faktor Authentifizierung

Sicherer Zugang zum Account



AIRBNB IS LATE TO THE MULTI-FACTOR PARTY THE VERGE

Airbnb adds new security measures to prevent scammers from hijacking hosts

By Nick Statt | @nickstatt | Apr 14, 2017, 5:37pm EDT

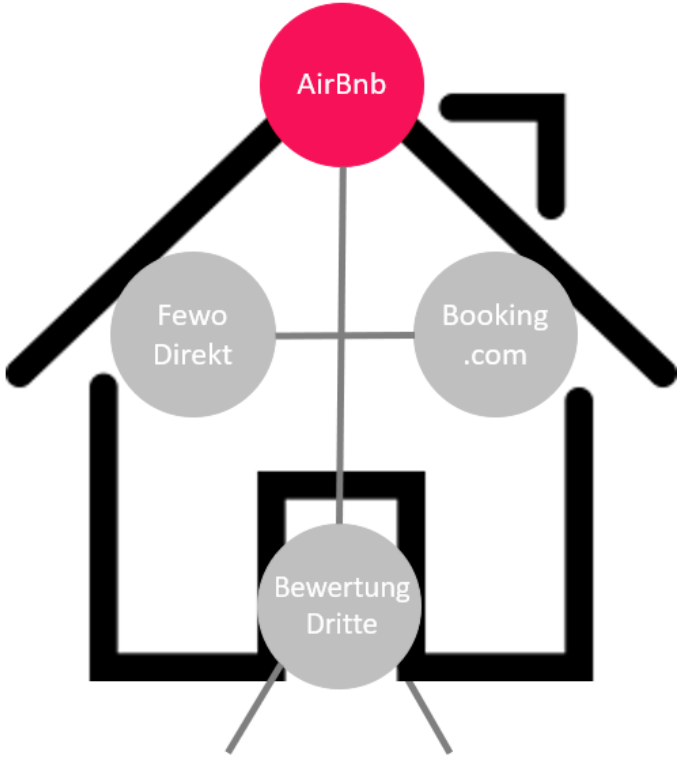
SHARE

3. Umsetzung der Anforderung

Technische Anforderungen: Sichere Datenspeicherung und keine Veränderung durch Dritte

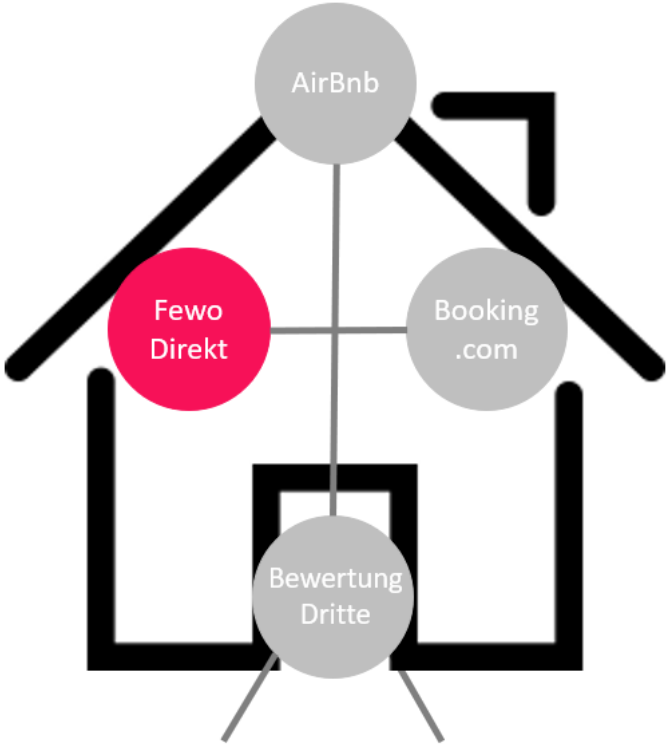
Stakeholder: Mieter, Vermieter

Sichere Datenspeicherung und keine Veränderung durch Dritte



➔ **Nahezu die gesamten Cloud Computing Funktionen laufen über AWS**

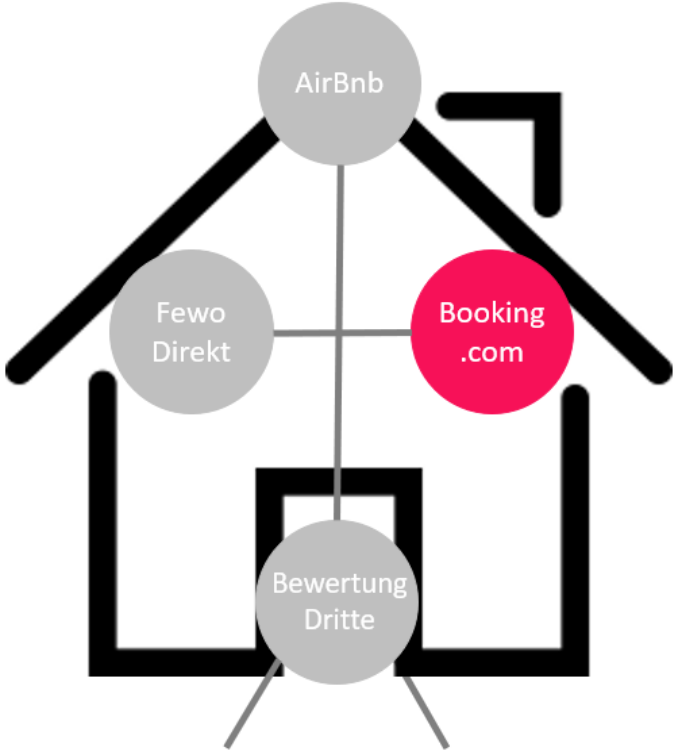
Sichere Datenspeicherung und keine Veränderung durch Dritte



Datenübermittlung in andere Länder

- ➔ **Angemessene Schutzmaßnahmen getroffen**
- ➔ **Bleiben geschützt wenn sie in andere Länder außerhalb des EWR übermittelt werden**
- ➔ **Stellen sicher, dass dritte Dienstleister, an die Daten übermittelt werden, angemessene Schutzmaßnahmen getroffen haben**

Sichere Datenspeicherung und keine Veränderung durch Dritte



Angemessene Abläufe

➔ **Für den Schutz ihrer personenbezogenen Daten vor Missbrauch und unberechtigtem Zugriff**

Sicherheitsverfahren

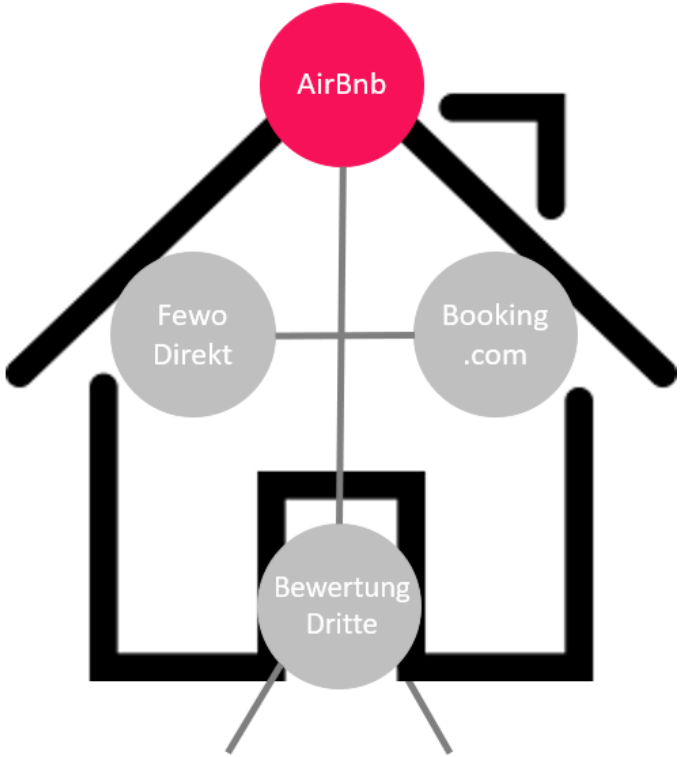
➔ **Technische Maßnahmen und Zugangsbeschränkungen**

3. Umsetzung der Anforderung

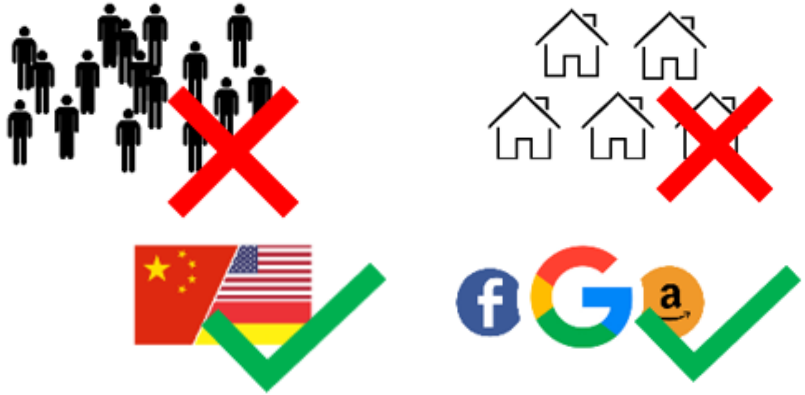
Datenschutz: Daten werden nur für den jeweiligen Zweck verwendet

Stakeholder: Mieter, Vermieter

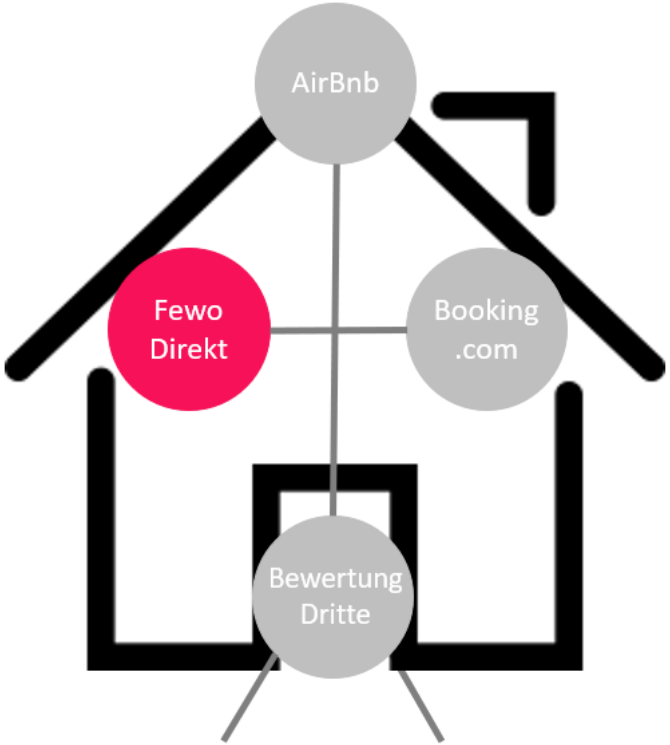
Daten werden nur für den jeweiligen Zweck verwendet



"Vielen Dank, dass Sie Airbnb nutzen! Ihr Vertrauen ist uns wichtig und wir verpflichten uns, die Privatsphäre und die Sicherheit Ihrer personenbezogenen Daten zu schützen. Die Informationen, die mit uns geteilt werden, helfen uns, Ihnen eine großartige Erfahrung mit Airbnb zu bieten. Wir haben ein engagiertes Datenschutzteam, das sich dem Schutz aller von uns erhobenen personenbezogenen Daten verschrieben hat und dazu beiträgt, dass personenbezogene Daten weltweit ordnungsgemäß behandelt werden."



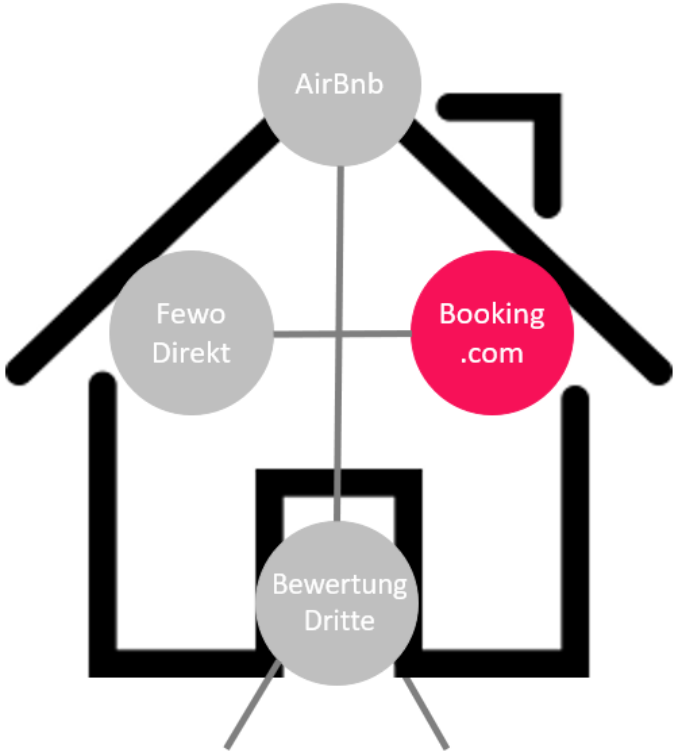
Daten werden nur für den jeweiligen Zweck verwendet



FeWo-direkt®
Teil der **HomeAway Familie**

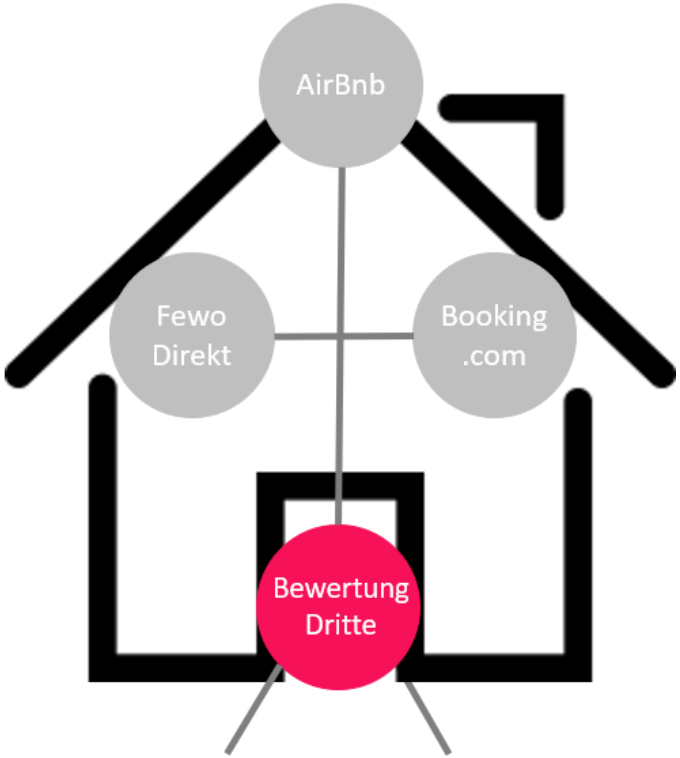
airbnb

Daten werden nur für den jeweiligen Zweck verwendet



“Das Wichtigste zuerst: Der Schutz Ihrer Privatsphäre liegt uns am Herzen. Uns ist bewusst, dass in allen diesen Bestimmungen so etwas in dieser Art steht, aber wir meinen es aufrichtig…”

Daten werden nur für den jeweiligen Zweck verwendet



Ach‘ Du schöne Ferienzeit.. Ausweiskopien bei Airbnb und das Recht auf Vergessenwerden

Unter dem Vorwand der Verifizierung werden sensible Daten abgefischt

Dass Airbnb jede Menge Daten sammeln will, um ein möglichst spezifisches Bild der Kunden zu bekomm ich nachvollziehen. Warum Menschen einem Unternehmen in den USA persönliche Daten in einer Qualit Verfügung stellen, die für einen Identitätsdiebstahl geradezu prädestiniert sind, bleibt mir ein Rätsel.

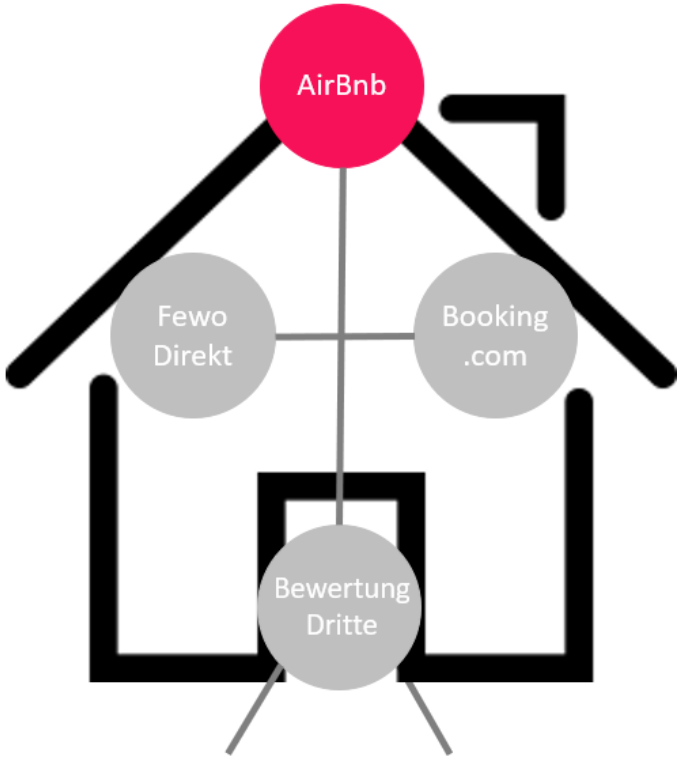
Bislang war die Buchung über Airbnb relativ unkompliziert und es war nachvollziehbar, warum bestimmt

3. Umsetzung der Anforderung

Betrugs- & Missbrauchsprävention: Profile/ Identitäten sind verifiziert bzw. überprüft

Stakeholder: Mieter, Vermieter

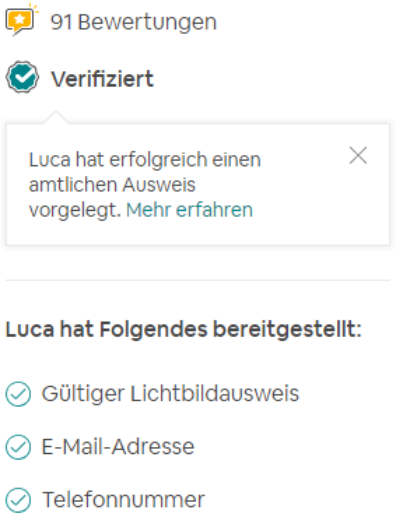
Profile/ Identitäten sind verifiziert bzw. überprüft



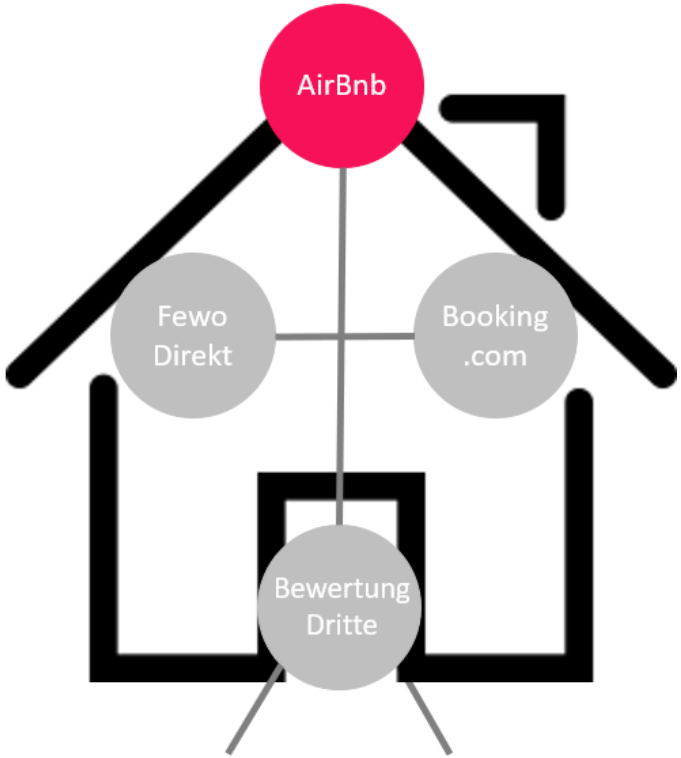
- **Pflichtangaben** bei Buchung einer Unterkunft:
  - vollständiger Name
  - Geburtsdatum
  - Telefonnummer
  - Mail-Adresse
  - Zahlungsdaten
- **optional**:
  - Ausweisdokument

⇨ verifiziertes Profil

- Abgleich mit Behörden-, Terroristen- und Sanktionslisten



Profile/ Identitäten sind verifiziert bzw. überprüft



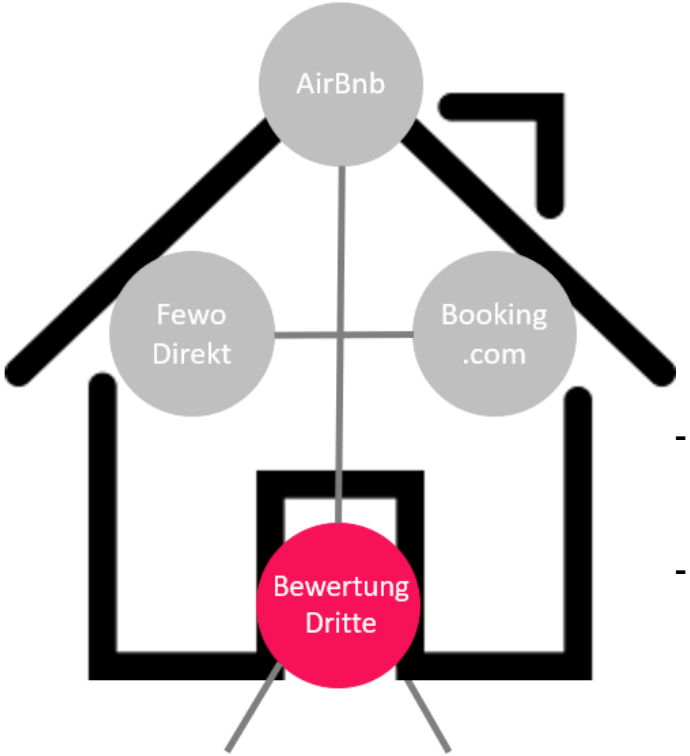
AGB von AirBnb:
"[…] dass ein Mitglied „verifiziert" wurde […] zeigt nur an, dass das Mitglied ein entsprechendes Verifizierungs- oder Identifizierungsverfahren abgeschlossen hat. Diese Beschreibung stellt keine Empfehlung, Zertifizierung oder Garantie seitens Airbnb in Bezug auf ein Mitglied, dessen Identität, Hintergrund, Vertrauenswürdigkeit, Sicherheit oder Eignung dar."

➔ **Identität wird nicht garantiert, keine staatliche Überprüfung**

Hilfe-Artikel von AirBnb:
"[…] können wir letztlich bei Nutzern, die außerhalb der USA leben, möglicherweise keine Überprüfung durchführen."
"Du solltest dich auch nicht auf Hintergrundprüfungen verlassen […]"

➔ **Überprüfung in den USA am zuverlässigsten**
➔ **im Allgemeinen keine Garantie für Überprüfung bzw. Zuverlässigkeit dieser**

Profile/ Identitäten sind verifiziert bzw. überprüft



- AirBbnb versucht, Profile zu filtern
- über unrechtmäßige Sperrung wird selten debattiert

Beispiel für Sperrung von Konto mit Verdacht auf Rechtsextremismus:

airbnb

Airbnb Customer Experience

Alex Z, Aug 5, 11:18 CDT:

Hi Mark,

After a routine review of your Airbnb account, we regret to inform you that we're no longer able to support your account due to a violation of our Terms of Service.

You can review our Terms of Service at: **www.airbnb.com/terms**

Reservation HMKDJCRB8J has been canceled for a full refund, and all other parties have been notified. Your refund should be reflected on your account within 5-7 business days, depending on your bank's processing time. This reservation will not be reinstated.

Per our Terms of Service, Airbnb reserves the right to make the final determination with respect to such matters, and this decision will not be reversed. For more information about account deactivations, visit **https://www.airbnb.com/help/article/432**

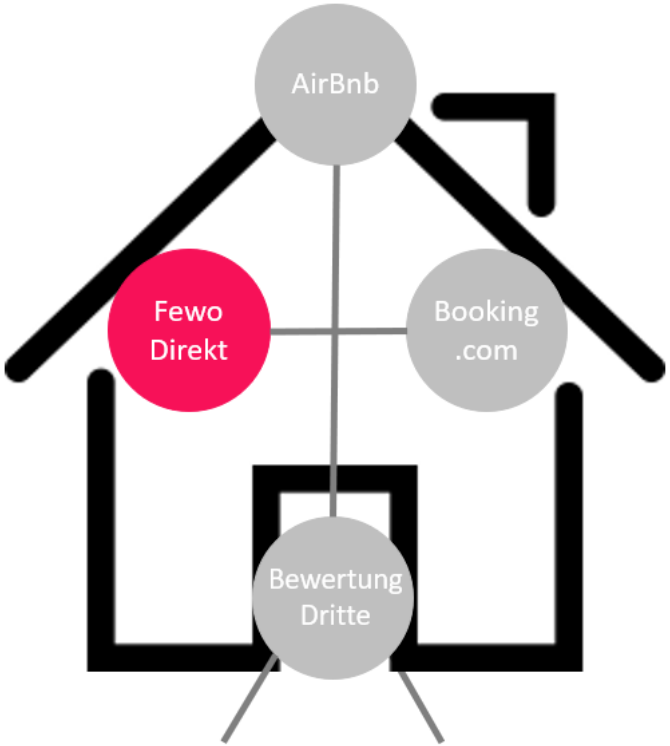
Best,

Alex
www.airbnb.com/help

THIS EMAIL IS A SERVICE FROM AIRBNB CUSTOMER EXPERIENCE.

Bildquelle:
https://twitter.com/Illegal_Aryan/status/893995780457078784/photo/1

Profile/ Identitäten sind verifiziert bzw. überprüft



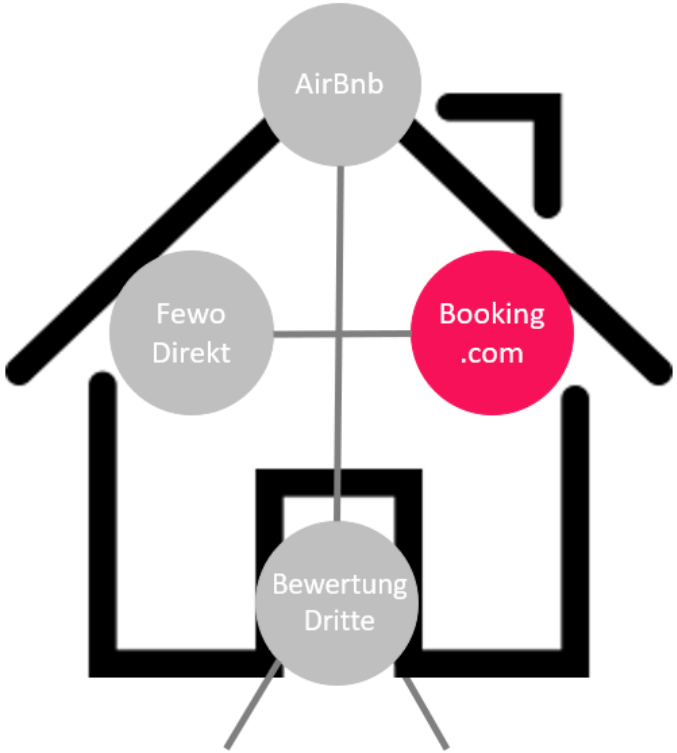
AGB von FeWo Direkt:
"Wir können […] keine Verantwortung dafür übernehmen, dass es sich bei einem anderen Nutzer tatsächlich um die von diesem Nutzer angegebene Person handelt."
"Sie bestätigen, dass HomeAway für die Überprüfung der Identität, für das Verhalten von Vermietern oder für die Überprüfung von Existenz, Art und Zustand der jeweiligen Unterkunft nicht verantwortlich ist"

FeWo-direkt
Teil der HomeAway Familie

=

airbnb

Profile/ Identitäten sind verifiziert bzw. überprüft



- **Profile sind nicht “verifiziert”, jedoch:**

Hilfe-Seite von Booking.com:
“Die Anbieter sind professionelle Anbieter in einem Vertragsverhältnis mit Booking.com. Ein Vertragsbruch bezüglich der Verpflichtungen des Anbieters gegenüber Booking.com kann dazu führen, dass der Anbieter auf der Website nicht mehr angezeigt wird.”

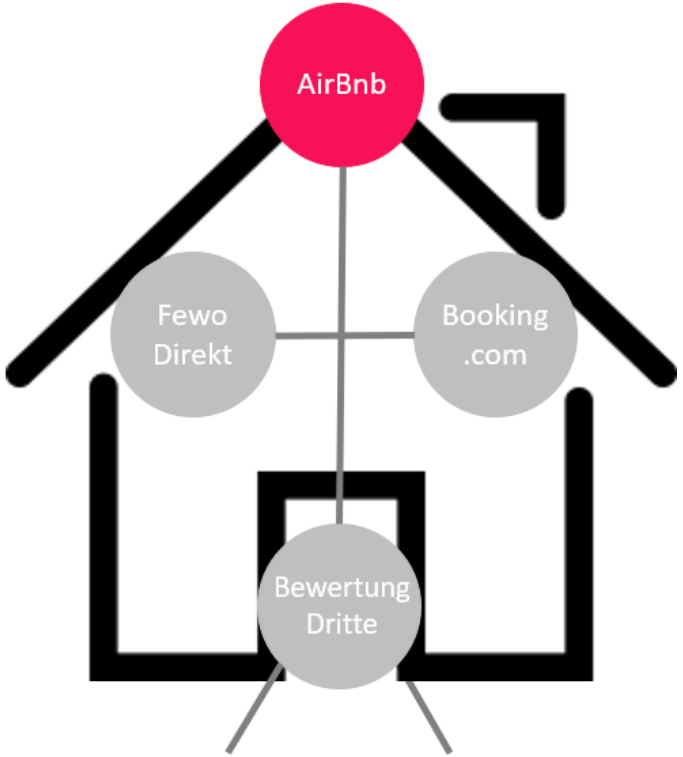
3. Umsetzung der Anforderung

Betrugs- & Missbrauchsprävention:

Schutz der Privatsphäre, vor Betrug und Schäden während des Besuchs

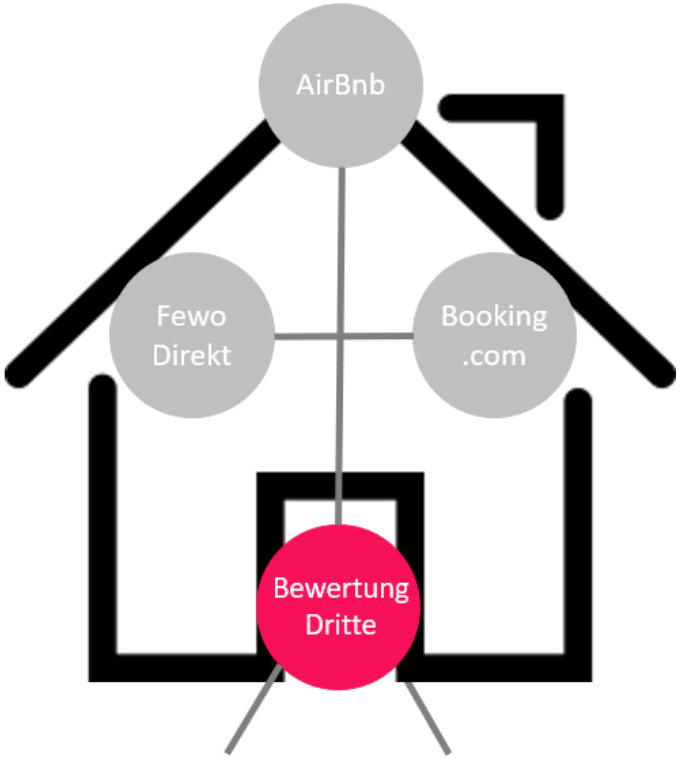
Stakeholder: Mieter, Vermieter

Schutz der Privatsphäre, vor Betrug und Schäden während des Besuchs



- **Risikobewertung** mit Hilfe von Vorhersagemethoden und maschinellem Lernen
- **Community-Standards** beschreiben Verhaltenskodex
- **Kundenservice 24/7** in elf verschiedenen Sprachen
- Gastgeber-Garantie & **Versicherung** zum Schutz von Gastgebern

Schutz der Privatsphäre, vor Betrug und Schäden während des Besuchs



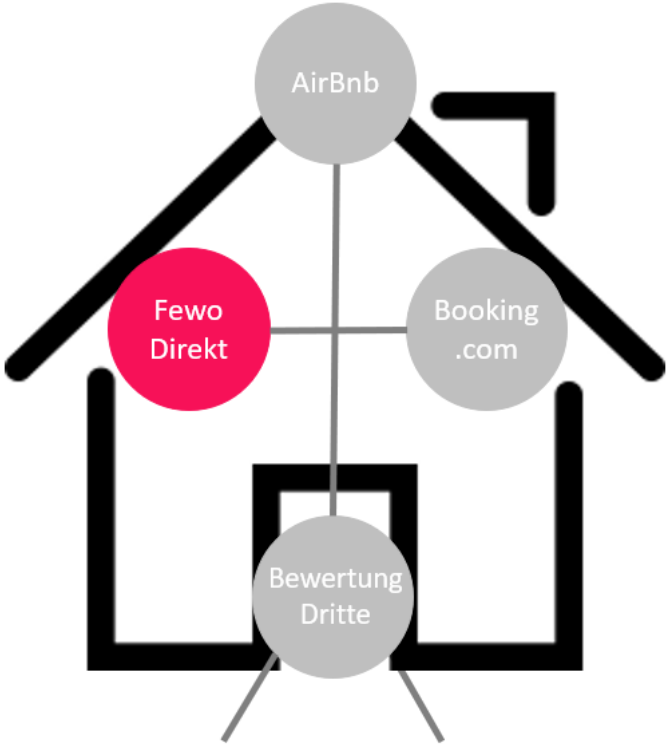
- ➔ Matching-Algorithmus beachtet …
- a) … Vorlieben, Geschmäcker etc. des **Gastes**
- b) … Faktoren, welche die Entscheidung des **Hosts** beeinflussen (z.B. Maximalbelegung, Zeitpunkt, Anzahl der Gäste)
- ➔ explizit von Risiko ist an der Stelle keine Rede

- ➔ Community-Standards werden mitunter missachtet

- ➔ Kundenservice funktioniert bei kleineren Anliegen gut

- ➔ ersetzt keine Haftpflichtversicherung (höhere Mindestabsicherung sinnvoll)
- ➔ unklar, wann die Absicherung genau wirkt

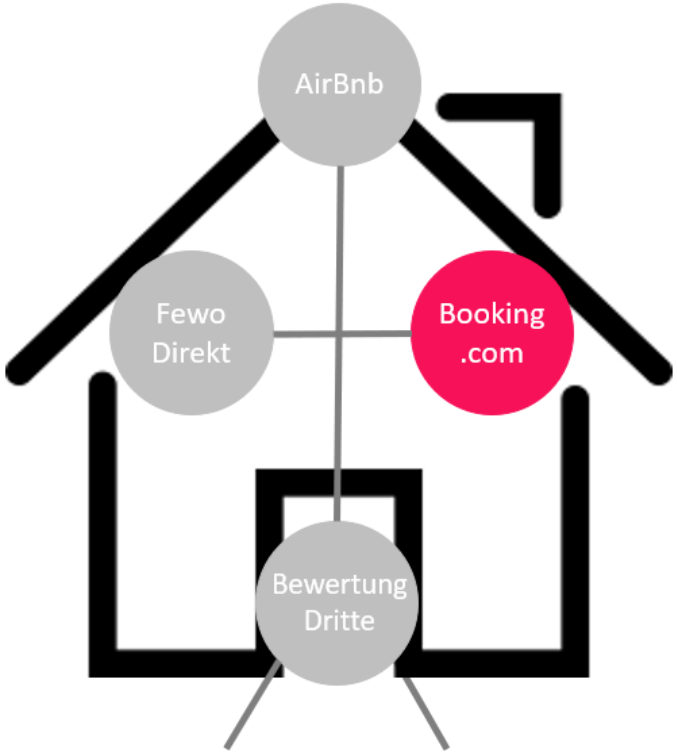
Schutz der Privatsphäre, vor Betrug und Schäden während des Besuchs



AGB von FeWo Direkt:
"Die Website dient lediglich als Marktplatz, auf dem Nutzer miteinander kommunizieren können. ***Mietverträge werden allein zwischen dem Urlauber und Vermieter geschlossen.*** *HomeAway ist und wird nicht Partei etwaiger vertraglicher Beziehungen zwischen Urlaubern und Vermietern und tritt im Falle von Streitigkeiten zwischen Urlaubern und Vermietern auch nicht als Vermittler auf."*

- ➔ **FeWo Direkt ist im Falle von "Streitigkeiten" aus dem Schneider**
- ➔ **Empfehlung: den Vermieter kontaktieren oder Beschwerde bei FeWo Direkt einreichen**

Schutz der Privatsphäre, vor Betrug und Schäden während des Besuchs



AGB von Booking.com:
"Ab dem Zeitpunkt Ihrer Reisebuchung wirken wir ausschließlich als Vermittler zwischen Ihnen und dem Reiseanbieter"
[...]
"Sie bestätigen und stimmen zu, dass der jeweilige Reiseanbieter alleinig für die Reise verantwortlich und haftbar ist. [...] Booking.com ist nicht verantwortlich (und lehnt jede Haftung ab) für jegliche Beschwerden, Ansprüche oder (Produkt-) Haftungen."

➔ **auch Booking.com ist nicht verantwortlich für jegliche Beschwerden**

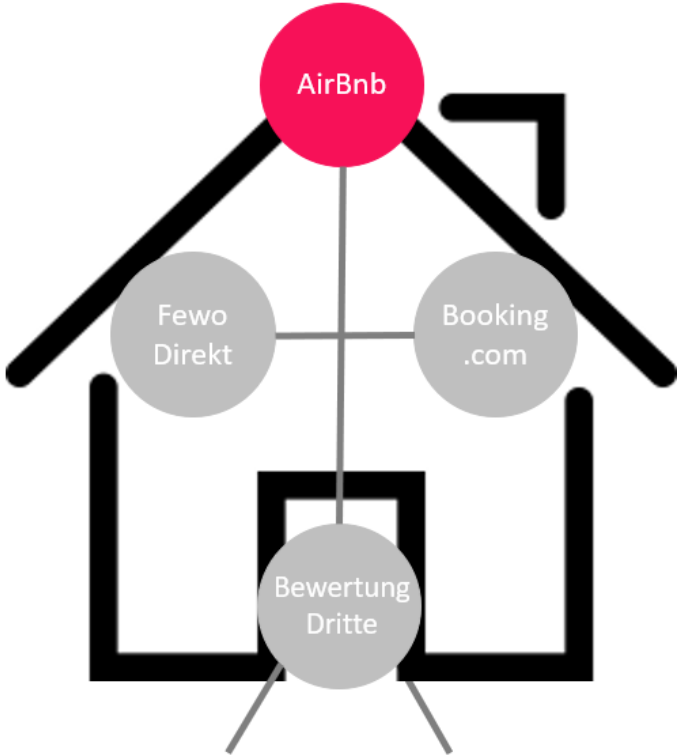
3. Umsetzung der Anforderung

Betrugs- & Missbrauchsprävention:

Überprüfung der Unterkünfte auf Richtigkeit aller Angaben

Stakeholder: Mieter, Vermieter

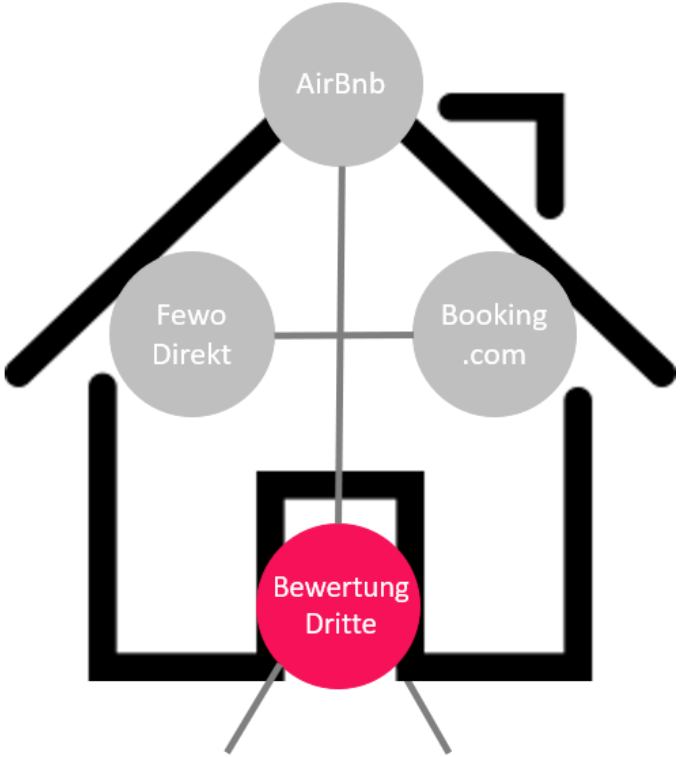
Überprüfung der Unterkünfte auf Richtigkeit aller Angaben



AGB von AirBnb:
"[AirBnb] […] kontrolliert und garantiert […] nicht (i) die Existenz, Qualität, Sicherheit, Eignung oder Rechtmäßigkeit von Inseraten oder Gastgeber-Diensten, (ii) die Richtigkeit oder Genauigkeit von Inseratsbeschreibungen, Bewertungen, Rezensionen oder sonstigen Mitglieder-Inhalten"

➔ **Empfehlung: Gastgeber, oder als zweite Instanz, AirBnb kontaktieren, falls etwas nicht den Erwartungen entspricht**

Überprüfung der Unterkünfte auf Richtigkeit aller Angaben



- extremes Negativbeispiel: **2655€ !**

➔ Folge der nicht flächendeckenden Kontrolle

Frankfurter Allgemeine

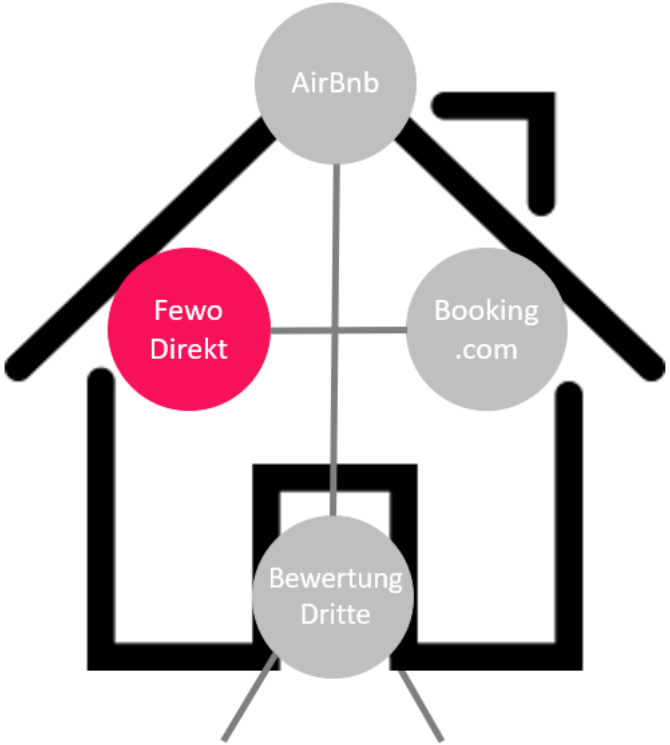
ONLINE-WOHNUNGSVERMITTLUNG

Wie Maya und Co. bei Airbnb tricksen

VON PETRA KIRCHHOFF, FRANKFURT
AKTUALISIERT AM 30.11.2015 - 22:04

Auf dem Portal des Bettenvermittlers stoßen Reisende immer wieder auf Schummel-Inserate. Ein Bad Homburger ist bei der Suche nach einem Quartier in St. Anton hereingefallen und kämpft jetzt um 2655 Euro.

Überprüfung der Unterkünfte auf Richtigkeit aller Angaben



AGB von FeWo Direkt:
"Inhalte fallen unter die Verantwortung der Vermieter […]. Wir ***übernehmen keine Verantwortung für die Inhalte****, da unsere Leistung darauf beschränkt ist Ihnen den Zugriff auf die Inhalte zu ermöglichen und Ihnen die Möglichkeit gewähren, sich direkt mit dem Vermieter in Verbindung zu setzen"*

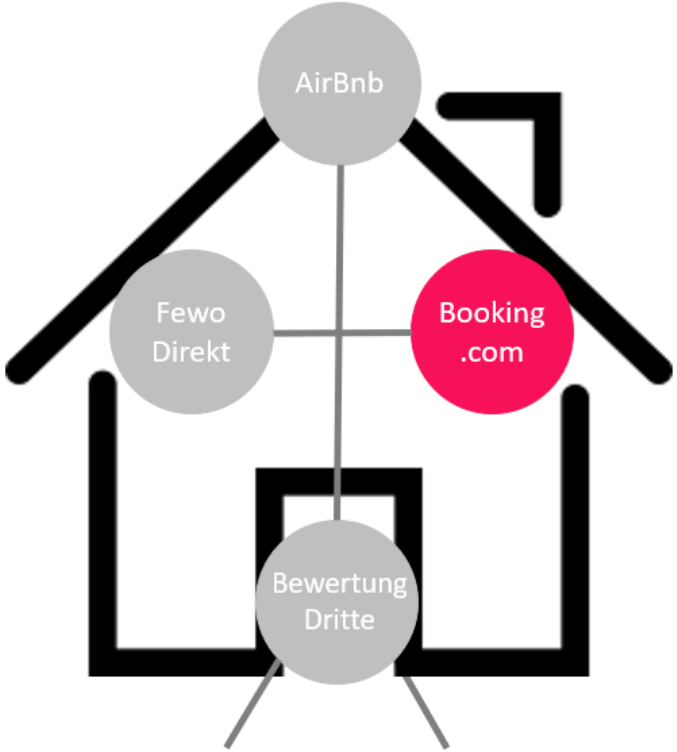
➔ **auch FeWo Direkt garantiert die Richtigkeit der Angaben nicht**

FeWo-direkt
Teil der HomeAway Familie

=

airbnb

Überprüfung der Unterkünfte auf Richtigkeit aller Angaben



AGB von Booking.com:
"[Wir können] weder überprüfen und garantieren, dass alle Informationen genau, richtig und vollständig sind, noch können wir für Fehler […], Unterbrechungen […], ungenaue, fehlleitende oder unwahre Informationen oder Nichtübermittlung der Informationen verantwortlich gemacht werden."

- ➔ **auch Booking.com garantiert die Richtigkeit der Angaben nicht**
- ➔ **Reiseleiter für Informationen verantwortlich**

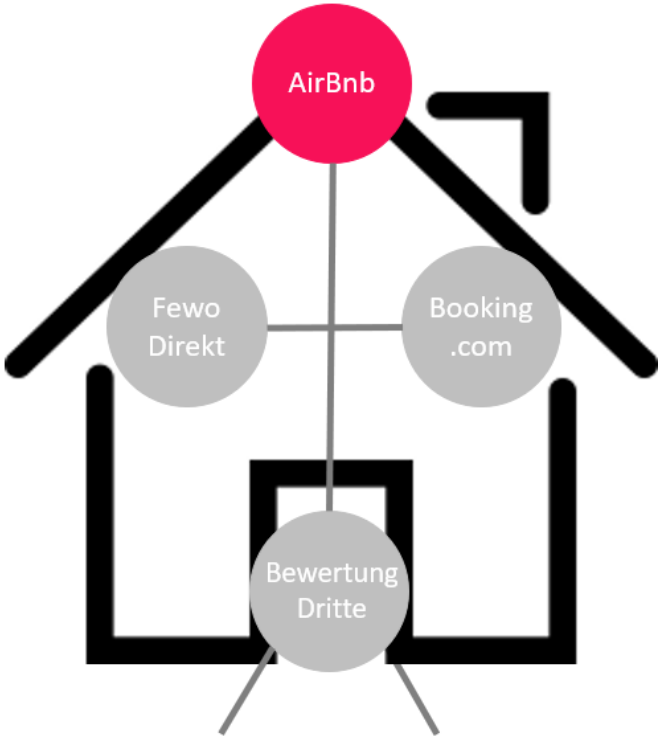
B. = FeWo-direkt Teil der HomeAway Familie = airbnb

3. Umsetzung der Anforderung

Sichere Zahlungen: Sichere Zahlungsarten und Transaktionen

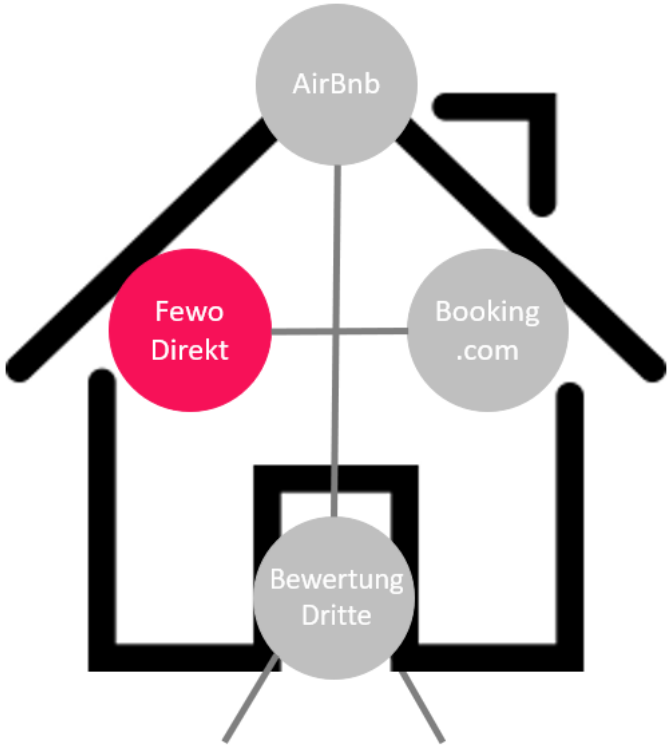
Stakeholder: Mieter, Vermieter

Sichere Zahlungsarten und Transaktionen



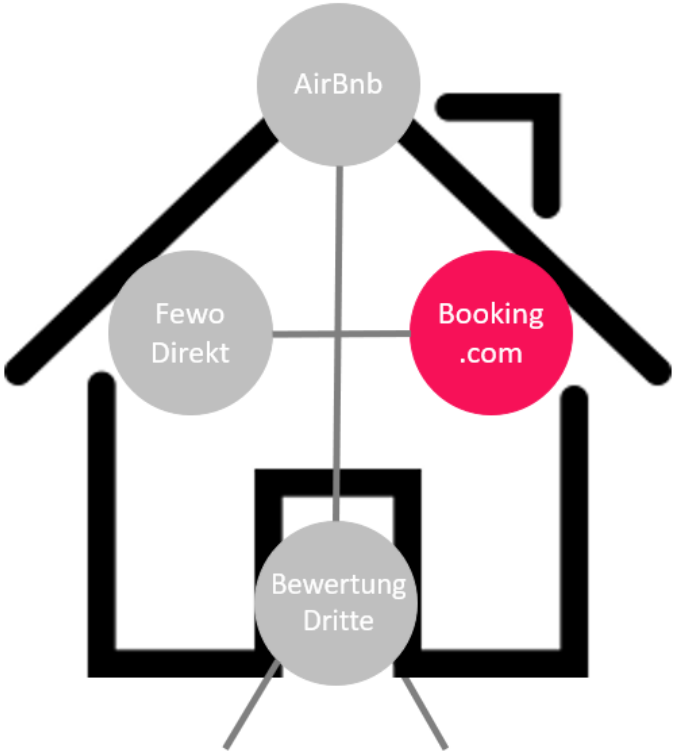
- ➔ Kreditkarten, Debitkarten, Überweisung, Paypal, Apple Pay, Google Pay, Alipay, Airbnb-Geschenkkarten, Coupons,
- ➔ Transaktionen sind über Airbnb abgesichert **“Kommuniziere & zahle immer über Airbnb”**
- ➔ Transaktionen werden durch jeweiligen Zahlungsanbieter erbracht

Sichere Zahlungsarten und Transaktionen



- ➔ Kreditkarten, Überweisung, Paypal, eCheck
- ➔ Transaktionen über “Mit-Vertrauen-Buchen-Garantie” abgesichert, wenn **über FeWo-direkt** gebucht bzw. gezahlt wird
- ➔ Systeme/Infrastruktur unterliegen strengen Sicherheitsanforderungen
- ➔ **PCI-DSS** (Payment Card Industry Data Security Standard) kompatibel

Sichere Zahlungsarten und Transaktionen



- ➔ Kreditkarten, Debitkarten, Überweisung, Paypal, Alipay, WeChat Pay, Geschenkkarten
- ➔ Keine Angaben über sichere Zahlungsabwicklung auf Booking.com
- ➔ In AGBs verweis auf jeweilige Zahlungsmethode und Anbieter
- ➔ Transaktionen werden vom jeweiligen Zahlungsanbieter erbracht und technisch abgesichert

Sicherer Zugang zum Account	
Sichere Datenspeicherung & keine Veränderung durch Dritte	
Daten werden nur für den jeweiligen Zweck verwendet	
Profile/Identitäten sind verifiziert bzw. überprüft	
Schutz der Privatsphäre, vor Betrug und Schäden während des Besuchs	
Überprüfung der Unterkünfte auf Richtigkeit aller Angaben	
Sichere Zahlungsarten und Transaktionen	

4. Architektur der Plattform

Architektur der Plattform

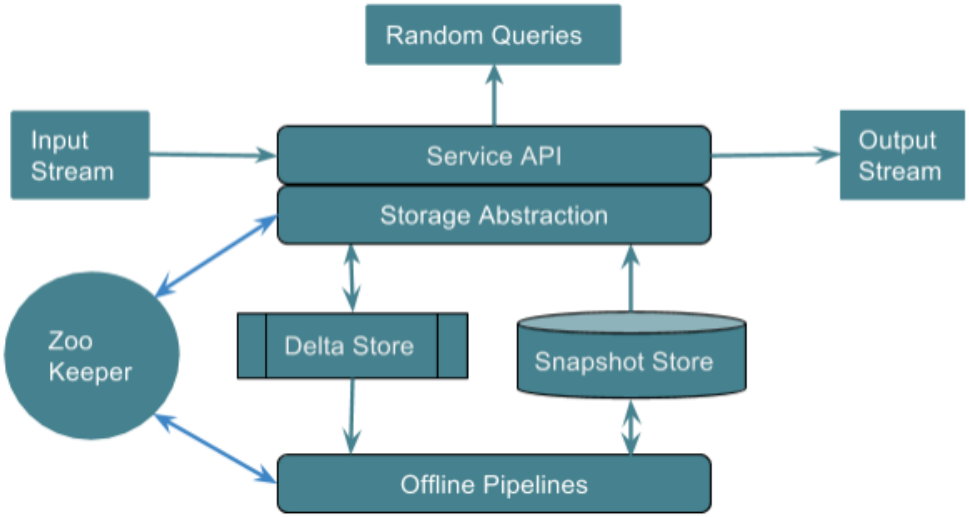
Aufbau der Gesamtarchitektur

Fokus auf zwei Modellen:

- **Datenaustauschmodell**
- **Dateninfrastruktur**

Architektur der Plattform

Datenaustauschmodell von AirBnB



- Verwendung von Nebula als Datenspeicherdienst
- Verwendung von DynamoDB als dynamischer Speicher
- Beide Speicher bedienen Read-Queries
- Nur dynamischer Speicher akzeptiert Write-Requests
- Koordination der Datenspeicher übernimmt Zookeeper

Architektur der Plattform

Nebular als Datenspeicherdienst

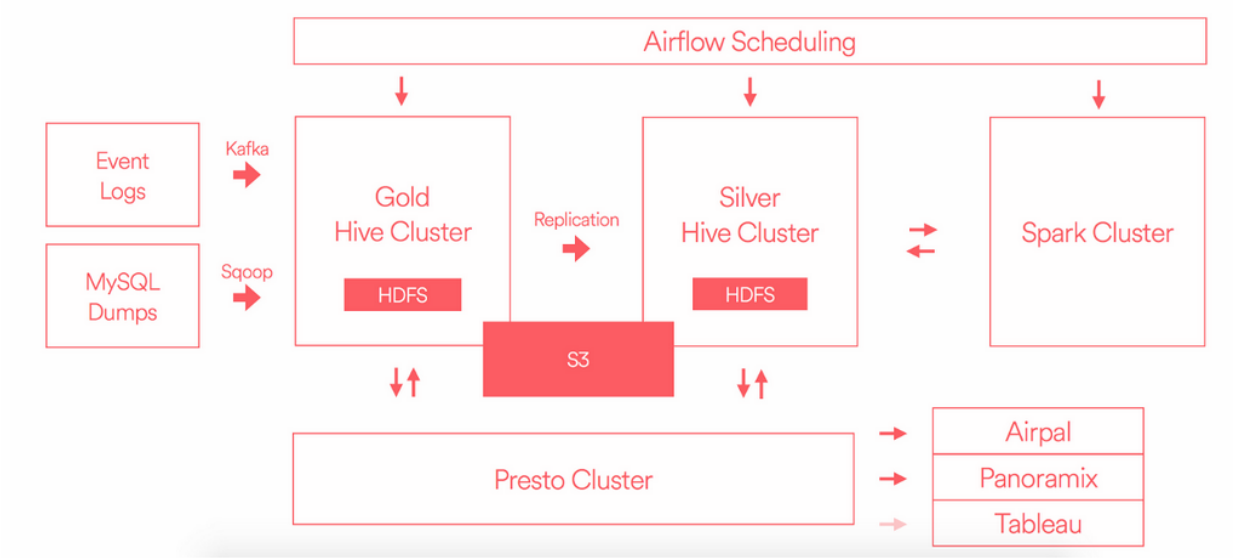
- Nebula bietet einheitliche API für die zugrunde liegenden physischen Speicher

- API wird als generische “key-value-store”-API bereitgestellt

- Nebula bietet definierte Schnittstellen an, über die Benutzer ihre Daten automatisch in das System laden können

Architektur der Plattform

Dateninfrastruktur



5. Technische Details der Plattform

Sicherheitskritische Betrachtung

Informationen zur Domain

Domain:	airbnb.com
Registriert in:	Kalifornien, USA
Registriert am:	2008-08-05
IP:	151.101.53.254
IP Location:	Kalifornien - San Francisco - Fastly
Hosting Company:	Fastly Edge Cloud-Platform
	Content Delivery Network (CDN), Bildoptimierung, Video- und Streaming-Dienste, Cloud-Sicherheit und Lastausgleichsdienste
Cloud-Sicherheitsdienste:	DDoS-Schutz (Distributed Denial of Service), Bot-Abwehr, Webanwendungs-Firewall
Hosting Provider:	Amazon
Server:	Amazon AWS
Server Standort:	Virginia, Ashburn, USA

Fakten zu Skripts, Cookies, Trackern

Skripts:

Anzahl der Scripts (gesamt):	120
Anzahl der Scripts (intern):	74
Anzahl der Scripts (extern):	46

Cookies:

First-Party:	20
Third-Party:	14

Tracker:

Third Parties Tracker:	28 (www.google-analytics.com, ad.doubleclick.net, a0.muscache.com, analytics.twitter.com, www.facebook.com etc.)
Third-party Anfragen:	223 Anfragen zu 28 eindeutigen Hosts

Zusammenfassung - Positive Aspekte

Verbindung und Verschlüsselung:

HTTPS-Verbindung:	vorhanden
SSL-Verschlüsselung:	vorhanden (unterstützt: TLS 1.2, TLS 1.1, TLS 1.0)
SSL-Zertifikat:	gültig
Aussteller:	DigiCert SHA2 Extended Validation Server CA
Gültig von:	31.05.2018
Gültig bis:	04.06.2020
Schlüssel:	RSA mit einer Schlüssellänge von 2048 bits
Signaturalgorithmus:	SHA256 mit RSA

HSTS:

HTTP Strict Transport Security (HSTS):	vorhanden

Zusammenfassung - Positive Aspekte

Flash-Inhalte:	Keine Flash Inhalte gefunden
Limit Login Attempts:	vorhanden, verhindert Brute Force Angriffe
Geräteerkennung:	vorhanden, abgesichert durch Airlock - 2FA
Single Sign On:	vorhanden, bereitgestellt durch Google und Facebook
Server Version:	nicht sichtbar

Zusammenfassung - Negative Aspekte

SSL-Verschlüsselung: Keine Unterstützung für TLS 1.3

Content Security Policy (CSP): teilweise unsicher implementiert

Cookies: teilweise ohne Secure und HttpOnly Flag gesetzt

Subresource Integrity (SRI): nicht eingebunden

Referrer Policy: nicht gesetzt

Potentielle Sicherheitslücke

Content Security Policy (CSP) teilweise unsicher implementiert

```
https://ajax.googleapis.com https://*.g.doubleclick.net https://www.google.com
https://www.gstatic.com https://smartlock.google.com
```

Keine konsequente implementierung der Anweisungen **default-src 'self'** und **script-src 'self'**

Mögliche Auswirkung:
Durch die unsichere Implementierung von Content Security Policy (CSP), ist die Webseite anfällig für Cross-Site Scripting (XSS) und Clickjacking Angriffe.

Mögliche Lösung:
Content Security Policy mit einem Content-Security-Policy HTTP Header zu aktivieren:

```
<!doctype html>
<head>
  <meta http-equiv="Content-Security-Policy" content="default-src 'self'; script-src 'self'">
```

Potentielle Sicherheitslücke

Cookies teilweise ohne Secure und HttpOnly Flag gesetzt

Cookies: 34	**HttpOnly**	**Secure**	**SameSite**	
20 first-party:	**0**		**9**	**0**
14 third-party:	**7**		**3**	**0**

Mögliche Auswirkung:
Unsichere Cookies können über JavaScript ausgelesen werden.
Ermöglicht Zugriff auf z.B. persönlichen Daten von Benutzern in der aktuellen Session

Mögliche Lösung:

- **Secure-Flag** verwenden, um Ihre Cookies vor einer versehentlichen Übertragung über HTTP zu schützen.
- **HttpOnly-Flag** Verwenden um Session-Cookies vor bösartigem JavaScript zu schützen.
  z.B. Set-Cookie: DAS COOKIE; Path=/; **Secure; HttpOnly**

Potentielle Sicherheitslücke

Subresource Integrity (SRI) wurden nicht eingebunden

Externe Drittanbieter-Ressourcen wie z.B. Scripte können über HTTP oder mit relativen URLs geladen src="//..."

```
https://connect.facebook.net/de_DE/sdk.js
```

Mögliche Auswirkung:
Hierdurch kann nicht überprüft werden, ob diese Ressourcen ohne Manipulationen übertragen wurden.

Mögliche Lösung:
SRI einbinden, damit ein Vergleich mit einem kryptographischen Hash, der mit dem von einer aufgerufenen Ressource übereinstimmen muss, durchgeführt werden kann.

SRI einbinden, indem die **integrity** und **crossorigin** Attribute einem **script** oder **link** Tag hinzugefügt werden.

<**script** src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js" integrity="sha384-tsQFqpEReu7ZLhBV2VZlAu7zcOV+rXbYlF2cqB8txI/8aZajjp4Bqd+V6D5IgvKT" crossorigin="anonymous"></**script**>

Potentielle Sicherheitslücke

Referrer Policy nicht gesetzt

Referrer-Header auf Defaultvalue: **Referrer-Policy: no-referrer-when-downgrade** gesetzt.

Mögliche Auswirkung:
Hierdurch ist Referrer Header auslesbar. Webseiten und Dienste können somit Nutzer verfolgen und z.B. die Surfgewohnheiten inkl. privater, sensibler Daten, insbesondere in Kombination mit Cookies erfassen.

Mögliche Lösung:
Eine Referrer Richtlinie mit einem **<meta>** Tag im HTML Quelltext oder in den **<head>** Bereich setzen:

z.B.
<meta name="referrer" content="no-referrer">

z.B.
Referrer Richtlinie in den HTTP Header ein:
Referrer-Policy: no-referrer

Fazit - Sicherheitskritische Betrachtung

HTTPS-Verbindung:

+

SSL-Verschlüsselung:

+

Zwei Faktor Authentifizierung:

+

Limit Login Attempts:

+

Absicherung von Cookies:

-

Content Security Policy:

Scan Summary

C-

Host:	www.airbnb.de
Scan ID #:	10921154
Start Time:	May 26, 2019 7:48 PM
Duration:	11 seconds
Score:	45/100
Tests Passed:	8/11