

HOTELLERIE & BETRUGSPRÄVENTION

Fake Bookings in der Hotellerie

Erkennen. Verstehen. Verhindern.

Isabell Kunert

Head of Distribution, Data & Payment Solutions — MEININGER Hotels
Fachvorstand Distribution — HSMA

ABLAUF DER SESSION

Vier Schritte.

1

ERKENNEN

10 Min

2

VERSTEHEN

15 Min

3

VERHINDERN

15 Min

4

ENTSCHEIDEN

20 Min

Ziel — Muster erkennen. Rote Flaggen lesen. Richtig eskalieren.

PROBLEMRAHMEN

Kein Reservierungsproblem. Ein Schnittstellenrisiko.

Revenue

Kapazität blockiert. Forecast verfälscht.

Vertrauen

Echte Daten machen Phishing glaubwürdig.

Payment

Betrug läuft bis zum Check-in weiter.

GEMEINSAMES VOKABULAR

Vier Muster.

1

No Intention to Stay

Kapazität ohne Reiseabsicht

2

Data Harvesting

Buchungsdaten als Köder

3

Payment Manipulation

Gefälschte Zahlungslogik

4

In-House Fraud

Betrug bis zum Check-in

Wichtig — Ein Fall kann mehrere Muster kombinieren.

DIE BUCHUNGSSTRECKE

Fünf Schnittstellen.

1

OTA / Direkt

Fake-Mail, ungültige Karte

2

PMS / CRS

Doppelte Reservierung

3

Payment

Pre-Auth scheitert

4

Messaging

Phishing ändert Kontakt

5

Front Desk

Manuelle Ausnahme

Ansatzpunkt — Prüfen, bevor die Buchung als „bestätigt“ weiterläuft.

NEUE DIMENSION

KI verändert das Spiel.

Sprachfehler sind kein Warnsignal mehr.



Perfektioniert

Fehlerfreies Phishing im Namen bekannter Marken.



Automatisiert

Bots erzeugen Massen-Fake-Buchungen & Kartentests.



Schützt jetzt

Offizielle Kanäle + Zwei-Faktor-Authentifizierung.

MUSTER 1 / 4

No Intention to Stay

Buchung ohne echte Reiseabsicht.

Kapazität blockiert

Visa-Zweckbuchung

Verfälschter Forecast

MUSTER 2 / 4



Guest Profile

Payment Information

Reservation Hijacking

Echte Daten. Falsche Absicht.

Phishing

Urgency statt Legitimation

Marken- & Datenrisiko

MUSTER 3 / 4

Zahlungsbetrug

„Bitte bestätigen Sie Ihre Zahlung — sonst wird storniert.“

1

Trigger

2

Druck

3

Link

4

Abgriff

Betrug am Empfang.

Wenn der digitale Fall physisch wird.

Stop-Regel — Passt Identität, Zahlung und Buchung nicht zusammen: nicht improvisieren, eskalieren.

NACH DEM AUFENTHALT

Der Chargeback.

Ohne Nachweis keine Verteidigung.

ID & Karte dokumentieren

Änderungsprotokoll sichern

Meldeschein reicht NICHT

VOR ANREISE

Rote Flaggen.



Kontakt

Neue Nummer, externer
Zahlungslink



Verhalten

Viele Zimmer, kurzfristige Änderung



Zahlung

Karte nicht belastbar, Off-Platform



Daten

Fragt nach internen Details

Merksatz — Buchung, Kommunikation und Zahlung müssen zusammenpassen.

VERHINDERN

Drei Ebenen.

People

Training. Klare Stop-Regeln.

Process

Vor-Anreise-Prüfung. Incident-Pfad.

Systems

MFA. Rollenrechte. Monitoring.

Prävention nach Kanal.

Kanal	Top-Risiko	Prüfpunkt	Stop-Regel
OTA	Messaging-Missbrauch	Nachricht & Link prüfen	Keine Off-Channel-Zahlung
Direkt	Fake-Kontakt & Kartentest	Kontakt, Domain, Zahlung	Keine Bestätigung bei Bruch
Walk-in	Identitätsmissbrauch	ID, Karte, Buchung abgleichen	Check-in stoppen
Gruppen	Serienbuchung, Kapazität	Vertrag, Ansprechpartner	Manuelle Freigabe

Bei Zeitdruck oder unklaren Daten: immer verifizieren, nie ungeprüft bestätigen.

WENN ES PASSIERT

Response Playbook.

1

Einordnen

2

→ Stoppen

3

→ Prüfen

4

→ Eskalieren

5

→ Entscheiden

Der Fall.

SITUATION

- Ein Gast aus einem visapflichtigen Nicht-Schengen-Land bucht direkt 14 Nächte – passend zur Mindestdauer im Visa-Antrag.
- Er bittet sofort um eine schriftliche Hotelbestätigung, möchte aber erst „nach dem Visa-Termin“ zahlen.
- Im PMS fehlen vollständige Gästedaten; die Kreditkarte ist nur als Garantie hinterlegt.
- Nach Versand der Bestätigung werden Rückfragen langsam beantwortet und kurz vor Anreise soll kostenfrei storniert werden.

DISKUSSION

- Wie hätte man das verhindern können?
- Was spricht für echte Reise, was für Visa-Zweck?
- Was muss vor dem Versand der Bestätigung vorliegen?
- Wann bestätigen wir nur mit klaren Bedingungen?
- Was tun, wenn Zahlung oder Daten ausbleiben?

VON DER THEORIE ZUR PRAXIS

30 Tage.

WOCHE 1

Stop-Regeln

WOCHE 2

Kanal-Checks

WOCHE 3

Training

WOCHE 4

Monitoring

Nicht mehr Regeln. Bessere Entscheidungen im kritischen Moment.

ZUM MITNEHMEN

Drei Sätze.

1

Fake Bookings sind Prozessangriffe.

Keine Einzelfehler.

2

Echte Daten machen Betrug glaubwürdig.

Kontext zählt, nicht nur die Buchung.

3

Die beste Verteidigung: klare Stop-Regeln.

Verifizieren statt bestätigen.

Fragen?

Erfahrungen · offene Fragen · nächste Schritte

Isabell Kunert · MEININGER Hotels · HSMA