Brennpunkt: Booking.com #cybersecurity - HSMA-Webinar vom 29.11.2024

Follow-up Q&A

1. **Frage**: Wenn Payment by Booking nicht in Anspruch genommen wird, und Hotels die CC als ungültig melden, hat der Bucher 3x jeweils 24 Stunden Zeit, eine andere CC bereit zu stellen. Dadurch werden Verfügbarkeiten im Hotel bis zu 72 Stunden blockiert. Warum diese lange “Grace Period” ?

   Antwort: Wenn Sie eine Kreditkarte als ungültig markieren, Ihr Gast jedoch innerhalb von 24 Stunden keine aktualisierten Angaben übermittelt oder erneut ungültige Kreditkartendaten angibt, können Sie die Buchung bis 15:00 Uhr (Ortszeit Ihrer Unterkunft) am geplanten Check-in-Tag stornieren. Der Kunde hat lediglich zwei Versuche. Wir möchten hier den Interessen der Hotels einerseits und den Kunden andererseits Rechnung tragen - beide haben ein Interesse an Planungssicherheit. Hier finden Sie weiterführende Informationen zum Thema.

2. **Frage:** Booking.com garantiert bei Buchungen und bemüht sich, die Stornokosten einzuheben. Ihr gebt uns keine CC weiter. Aus Sicherheitsgründen, sagt ihr, ist dies nicht möglich

   Antwort: Der Umgang mit Kreditkartendetails basiert auf den für die Reservierung ausgewählten Richtlinien. Die von uns weitergegebenen Daten unterscheiden sich je nach Region und Richtlinie. Beispielsweise geben wir bei Zahlungen über Booking.com oder Hybridzahlungen über Booking.com die Kreditkartendaten nicht an den Partner weiter, da wir die Zahlung einziehen (ob vollständig oder teilweise, d. h. bei Nichterscheinen/Stornierung). Auch bei Pay at Property-Buchungen von Unterkünften im Hybridmodell geben wir Kreditkartendaten nicht weiter. Dies liegt daran, dass wir die Karten im Namen der Partner validieren und von deren Hälfte auch No-Show- und Stornierungsgebühren erheben. Insofern besteht für das Hotel keine Notwendigkeit, Kreditkartendaten zur Durchführung des Vertrages zu erhalten - auch aus datenschutzrechtlichen Gründen ist uns damit die Weitergabe der Kartendetails verwehrt.
   Weitere Informationen zum Thema Einsehbarkeit von Kreditkartendetails und Fehlerbehebung hier.

3. **Frage:** In der Vergangenheit hatten Hacker trotz 2-Wege-Authentifizierung Zugriff auf das Extranet. Diese zweite Sicherheitsinstanz sollte den Zugriff eigentlich vermeiden. Wurde dies behoben?

   Antwort: Angreifer können 2FA auf verschiedene Weise erlangen, zum Beispiel durch Phishing-Websites, Social Engineering oder Malware. 2FA ist eine gute Hürde für

Angreifer, kann jedoch umgangen werden, z.B. wenn Partner unbeabsichtigt Anmeldedaten und 2FA-PINs mit Angreifern teilen.

Es ist wichtig zu beachten, dass 2FA eine zusätzliche Sicherheitsebene bietet, aber nicht unfehlbar ist. Sie kann umgangen werden, insbesondere wenn Benutzer unbeabsichtigt ihre Anmeldedaten und 2FA-PINs mit Angreifern teilen. Daher ist es entscheidend, dass Benutzer auch andere bewährte Sicherheitspraktiken befolgen, wie die Verwendung starker und einzigartiger Passwörter, das regelmäßige Aktualisieren von Sicherheitssoftware und das Bewusstsein für Phishing-Angriffe.
Mehr Informationen dazu im Partner hub.

4. **Frage**: Zwei Factor Authentifizierung: Wieso wird die nicht immer vorgeschlagen bzw. abgefragt, also wieso ist es nicht verpflichtend bei jedem Login?

   Antwort: Wir möchten erhöhte Sicherheit und verbesserte Benutzererfahrung gewährleisten. Daher wird die Zwei-Faktor-Authentifizierung auf der Grundlage einer Risikoanalyse aktiviert: Verifizierungen werden nur bei verdächtigem Verhalten verlangt, wodurch der Aufwand für legitime Benutzer reduziert wird.

5. **Frage**: Wie weit ist man bei Booking.com mit einer Single Sign on-Option? Laut unserem Key Account Manager soll das irgendwann ausgerollt werden. Das wäre sicherer als die 2FA.

   Antwort: Wir arbeiten mit vollem Einsatz daran, unsere Sicherheitsmaßnahmen auf dem neuesten Stand der Technologie zu halten und weiter auszubauen, um Angriffen zu begegnen und sie zu bekämpfen. Mehr Informationen dazu finden Sie hier.

6. **Frage**: In allen Hotels, die ich unterstütze, bekommen wir meines Erachtens die Kreditkartendaten. Seit wann teilt Booking.com die nicht mehr? Oder ist das nur der Fall, wenn Booking das Inkasso macht?

   Antwort: Booking.com bietet verschiedene Zahlungsmöglichkeiten und Produkte an. Welche Produkte Sie verwenden, kann das Timing und die Übermittlung der Kreditkartendaten beeinflussen. Mehr Informationen hier und hier.

7. **Frage**: Gibt es ein Log bei Booking.com und wieso steht es den Admins im geschützten Bereich nicht zur Verfügung? So kann überprüft werden, ob Mitarbeiter die Passwörter wirklich geändert haben.

   Antwort: Im Moment sind diese Protokolle für den Partner nicht zugänglich. Das Hauptkonto und das Admin-Konto können Nutzerkonten verwalten. Hier haben Sie eine Übersicht über den letzten Anmeldetag des Benutzers. Mehr Informationen dazu finden Sie hier.

8. **Frage:** Zum Thema Machine Learning: Booking nutzt Machine Learning für die Betrugsprävention. Wie sieht es denn da mit dem Datenschutz aus?

   Antwort: Wir verwenden risikobasierte Authentifizierungs- und Zugriffsverwaltungskontrollen, die auch durch ML-Modelle unterstützt werden. Machine Learning hilft uns dabei, diese Prozesse effizient und sicher und im Einklang mit dem Datenschutz zu gestalten.

9. **Frage**: Wie transparent ist Booking.com bei der Weitergabe von Sicherheitsmaßnahmen und Hackerangriffen?

   Antwort: Wir arbeiten mit vollem Einsatz daran, unsere Sicherheitsmaßnahmen weiter auszubauen, um diesen Angriffen zu begegnen und sie zu bekämpfen. Wir informieren unsere Partner über unser Extranet, den Partnerhub und auch über Webinare. Bitte haben Sie Verständnis dafür, dass wir unsere technischen Maßnahmen nicht im Detail offenlegen können - wir würden Hackern sonst ggf. Angriffsflächen bieten.

10. **Frage**: Können Hacker die Booking.com-Mailadressen der Gäste auch später noch nutzen, obwohl die Systeme des Hotels nach dem Hackerangriff bereits wieder sicher sind, um Gäste aus der Sicht des Hotels anzuschreiben?

    Antwort: Nein. Wir ändern Alias-Email-Adressen je nach Ergebnis des Vorfallsberichts.

11. **Frage:** Gibt es nicht die Möglichkeit des Geoblocking? Also Zugriff nur aus dem Land, in dem der Account auch registriert ist? Kann über VPN umgangen werden, aber würde es komplizierter machen.

    Antwort: Wir priorisieren derzeit andere technische Verfahren, die uns auch im Hinblick auf die technischen Gegebenheiten unserer Unterkunftspartner effizienter erscheinen. Festzuhalten ist zudem, dass Cyberangriffen häufig aus dem gleichen Land erfolgen, in dem sich auch die Unterkunft befindet. Ein generelles Geoblocking wäre daher nicht zielführend.

Nachstehend noch einige Zusatzinformationen zu den im Webinar angesprochenen Themen sowie allgemein zum Thema Cybersecurity:

- Unsere Tipps für mehr Bewusstsein für Cybersicherheit liefern wertvolle Erkenntnisse zum Schutz Ihrer Unterkunft, Mitarbeitenden und Gäste vor Cyberbedrohungen.
- Zahlungsdiensterichtlinie (PSD2)
- Recht und Sicherheit
- Informationen des Bundesamtes für Sicherheit in der Informationstechnik (mit Sicherheitshinweisen/ als Anlaufstelle bei Cybersecurity-Vorfällen).