Berlin Commissioner
for Data Protection
and Freedom of Information

Berlin Commissioner for Data Protection and Freedom of Information
Alt-Moabit 59-61, 10555 Berlin, Germany

Herr Warnecke

Reference number:	Hauser
Department:	
Contact person:	
Telephone:	+49 30 13889-0
Extension:	
Date:	26. Januar 2024

Sehr geehrte Herr Warnecke,

Ihre E-Mail vom 18. Januar 2024 ist bei uns eingegangen.

Ihre Frage zur rechtlichen Einschätzung, ob der geschilderte Sachverhalt für betroffene Hotels zu einer Meldepflicht nach Art. 33 DS-GVO führen könnte, möchten wir wie folgt beantworten:

Zuerst möchten wir Sie auf Art. 33 Abs. 1 DS-GVO hinweisen:
Art. 33 Abs. 1 DS-GVO:
Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 55 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.

Von der niederländischen Aufsichtsbehörde, die für Booking.com zuständig ist, haben wir die folgende Ausführung für Betroffene erhalten:

> *„Booking.com nimmt zur Kenntnis, dass Sie möglicherweise einen Phishing-Vorfall erlebt haben und Bedenken hinsichtlich der Sicherheit Ihrer personenbezogenen Daten haben.*

Wir möchten erläutern, wie sich dies zugetragen haben könnte und möchten dafür sorgen, dass Sie die erforderliche Unterstützung und Absicherung erhalten.
Booking.com ist sich bewusst, dass eine Reihe seiner Unterbringungspartner (z. B. Hotels und Anbieter anderer Arten von Unterkünften) von Social Engineering, Phishing-Nachrichten und Schadsoftware ins Visier genommen werden, die dazu geführt haben könnten, dass ihre Systeme durch einen böswilligen Akteur für Zwecke des Online-Betrugs beeinträchtigt wurden. Dies kann zu unbefugtem Zugang zu ihrem booking.com-Konto führen, was einem unbefugten Dritten ermöglicht, zu versuchen, Zugang zu Buchungsdetails zu erhalten und/oder Missbrauch des Nachrichtenübermittlungssystems zur Übermittlung betrügerischer Meldungen zu betreiben (in einigen Fälle, einschließlich böswilliger Zahlungs-Links).
Bei diesem Szenario handelt es sich um eine Panne im System eines Unterbringungspartners oder um eine Panne im Konto, mit welchem der Beherbergungspartner seine Angebote auf booking.com verwaltet. Es ist aber keine Panne in den Backend-Systemen oder -Infrastrukturen von booking.com.
Wir verstehen Ihre Bedenken hinsichtlich des möglichen Schadens, der sich aus diesem Vorkommnis ergeben könnte. Obwohl die Panne nicht von booking.com ausging, unternimmt booking.com dennoch umfassende Maßnahmen zur Minderung des potenziellen Schadens aus solchen Online-Betrugsfällen für Kunden und Unterkünfte. Sobald booking.com Kenntnis davon erhält, dass ein Konto betroffen ist oder die Kunden Phishing-Nachrichten erhalten, untersucht booking.com das Problem rasch und ergreift manuelle und automatisierte Maßnahmen, um einzugreifen (z. B. Sperrung des Kontos). Außerdem benachrichtigt booking.com unverzüglich die Behörden, die betroffenen Unterkunftspartner und betroffene Kunden im Einklang mit dem Gesetz, sobald booking.com eine Verletzung des Schutzes personenbezogener Daten auf Seiten des Partners oder Kunden bestätigt und genauere Informationen hat.
Booking.com hält auch an einer Reihe sich regelmäßig weiterentwickelnder Sicherheits- und Betrugspräventions-/Erkennungsmaßnahmen zur Gewährleistung der Sicherheit ihrer Systeme bereit.
Diese Maßnahmen umfassen:
• Obligatorische 2FA-Zulassungskontrollen, die nicht nur ausgelöst werden, wenn der Unterkunftspartner sich in sein Konto einloggt, sondern auch dann, wenn Maßnahmen mit höherem Risiko getroffen werden (z.B. das Einsehen personenbezogener Daten);
• Ausstattung der Unterbringungspartner (die verschiedene Immobilien und/oder Teams an einem oder mehreren Orten verwalten) mit feinkörniger Authentifizierung und

Zugangskontrolle zu ihren booking.com-Konten, die das Risiko für Kunden, Opfer gezielter Betrugsversuche zu werden, verringern.
• Maßnahmen zur Aufdeckung gefälschter Buchungen, die es booking.com ermöglichen, proaktiv Buchungen zu annullieren, von denen angenommen wird, dass sie von einem böswilligen Akteur geltend gemacht werden (und als Teil eines Phishingversuchs gegen den Unterbringungspartner genutzt werden könnten);
• Betrugsbekämpfungsmaßnahmen auf der booking.com-Messaging-Plattform, die zum Beispiel Hyperlinks an unsere Kunden blockieren;
• Wiederkehrende Sensibilisierungskampagnen für Unterbringungspartner, um sie darin zu schulen, Angriffe im social engineering zu verhindern;
• Spezielle booking.com-Teams, die auf Prävention, Aufdeckung und Ermittlung von Online-Betrug spezialisiert sind, und Ermittlungen, die weltweit in mehreren geografischen Gebieten durchgeführt werden; und
• Automatisierte Sicherheitsüberwachung (mit der ungewöhnliche Zugriffe ermittelt und auf diese reagiert wird) und Datenminimierungspraktiken (die u.a. verhindern, dass Unterkunftspartner, Buchende direkt über ihre E-Mail-Adresse erreichen).
Als Verbraucher spielen Sie nach wie vor eine Schlüsselrolle, die Folgen von Online-Betrug auf ein Minimum zu begrenzen. Booking.com ermuntert Sie, wachsam zu bleiben und nicht auf ungewöhnlichen oder verdächtigen Aktivitäten zu antworten, einschließlich Zahlungsaufforderungen über WhatsApp.
Wenn Sie eine ungewöhnliche Aktivität im Zusammenhang mit einer Reservierung in einer Unterkunft feststellen oder Bedenken hinsichtlich der Sicherheit Ihrer personenbezogenen Daten habe, steht Ihnen booking.com über sein Hilfezentrum stets gerne zur Verfügung. “

Die bisher eingegangenen Meldungen bzgl. des Datenschutzvorfalls konnten noch nicht abschließend bewertet werden. Leider sind noch nicht alle Antworten von den meldenden Unternehmen eingegangen. Wenn die Schutzverletzung der personenbezogenen Daten beim IT-System des Hotels als Verantwortlichem passiert, dann ist das betroffene Unternehmen nach Art. 33 DS-GVO meldepflichtig. Dass die versendeten E-Mails wie E-Mails von booking.com aussehen, ist hier nicht entscheidend.

Als Berliner Beauftragte für Datenschutz und Informationsfreiheit stellen wir auf unserer Website und damit auch Ihnen und Ihren Mitgliedern für Ihre Meldung ein Formular sowie einen Link zu unseren Kontaktdaten zum Abruf bereit. Bitte beachten Sie auch unsere Hinweise

zum Ausfüllen des Meldeformulars, das Sie unter dem folgenden Linke finden: https://www.datenschutz-berlin.de/datenschutz/datenpanne/datenpannenformular/. Wenn andere Datenschutzaufsichtsbehörden zuständig sind, so sind die Meldewege der jeweiligen Behörden zu nutzen. Eine Übersicht finden Sie hier: https://www.bfdi.bund.de/DE/Service/Anschriften/Laender/Laender-node.html

Mit freundlichen Grüßen

gez. Hauser