CYBERVORFALL BEI BOOKING.COM

(STAND: Januar 2024)

Phishing-Angriff bei booking.com

Anfang Dezember 2023 berichtete *heise online*, dass Phishing-Angriffe zur Hotelbuchungsplattform *booking.com* bekannt geworden sind.

Link: https://www.heise.de/news/Phishing-Angriffe-Betrueger-missbrauchen-Hotelbuchungsplattform-booking-com-9547507.html

In der jüngsten Zeit wurden diesbezüglich mehrere Vorfälle als Datenpanne in Berlin gemeldet. Wir möchten Ihnen daher einige Informationen zu diesem Phishing-Angriff sowie Handlungsempfehlungen geben, um Schaden vom Hotel und vor allem von Ihren buchenden Gästen abzuwenden.

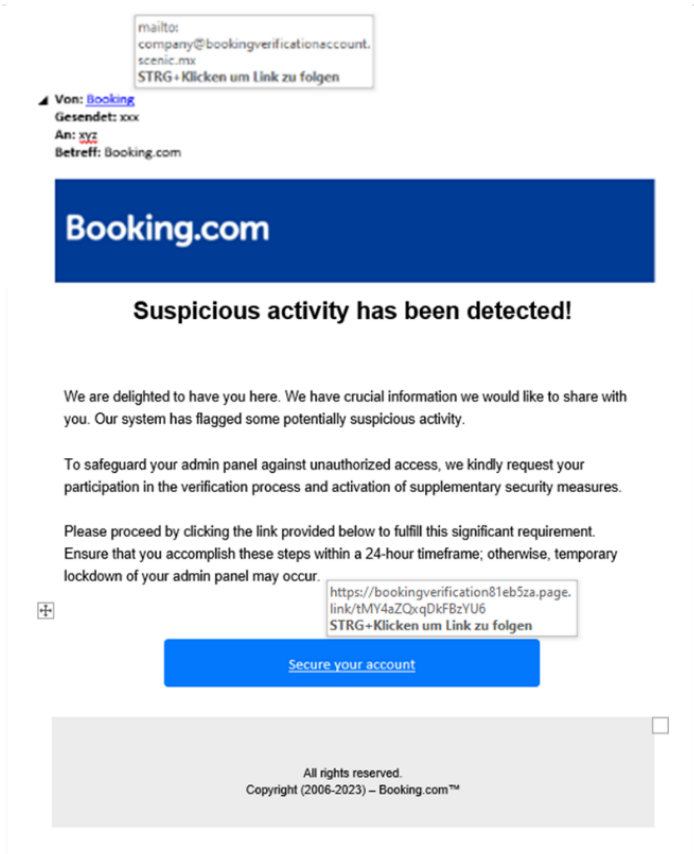
Was ist ein Phishing-Angriff?

Ein Phishing-Angriff ist eine betrügerische Methode, bei der versucht wird, vertrauliche Informationen wie Zugangsdaten (Benutzernamen, Passwörter) und Kreditkarteninformationen von Einzelpersonen oder Unternehmen zu stehlen. Der Angreifer gibt meist vor, ein vertrauenswürdiges Unternehmen oder Person zu sein, um das Opfer dazu zu bewegen, sensible Informationen preiszugeben.

Typischerweise erfolgt ein Phishing-Angriff über gefälschte E-Mails, Webseiten oder Nachrichten, die so gestaltet sind, dass sie authentisch aussehen. Die Opfer werden dann dazu verleitet, auf Links zu klicken, die zu gefälschten Webseiten führen. Auf ihnen werden sie aufgefordert, ihre persönlichen Daten einzugeben. Diese gefälschten Webseiten sehen oft täuschend echt aus, was es für den Betroffenen schwierig macht, sie von legitimen Seiten zu unterscheiden.

Wie läuft der Angriff bei booking.com?

Der erste Angriff erfolgt direkt im Hotel! Hierzu werden auf E-Mail-Adressen, welche auf der Webseite veröffentlicht sind (bspw. *info*@), Phishing Mails versendet. Siehe das Beispiel.



Der Empfänger wird aufgefordert, die Zugangsdaten zum Hotel-Account einzugeben. Bei den bekannten Fällen nutzten die Angreifer im Folgenden die Zugangsdaten, um sich Zugriff auf den Hotel-Account zu verschaffen. Dabei haben die Angreifer eine Möglichkeit gefunden, an der Zwei-Faktoren-Authentifizierung (2FA), welche durch *booking.com* i.d.R. erzwungen wird, vorbeizukommen.

WICHTIG

Bei jeder E-Mail ist zu prüfen, ob die E-Mail-Adresse des Versenders authentisch ist. Diese kann mit einem Mouseover angezeigt werden. Bewegen Sie hierzu den Mauszeiger über einem bestimmten Bereich (Absender) auf der E-Mail. Gleiche Prüfung gilt für jeden Link in einer E-Mail.

Klicken Sie nie ungeprüft auf einen Link!

Was passiert, wenn die Angreifer im Hotel-Account bei booking.com sind?

Die Angreifer schreiben aus dem Hotel-Account heraus den Gast direkt über *booking.com* an, welcher kürzlich eine Buchung durchgeführt hat. Er wird darum gebeten, über einen bereitgestellten Link die persönlichen Daten zu vervollständigen und die Buchung über seine Kreditkarte zu verifizieren. Anderenfalls ist die Buchung nicht garantiert und wird storniert. Ihnen wird hierzu i.d.R nur ein Zeitfenster von 12 Stunden gelassen.

Die Buchenden erhalten eine E-Mail im Namen des Hotels direkt aus dem System von *booking.com.* Sie vertrauen bei der Kommunikation auf die Richtigkeit des Inhaltes. Im Hotel-Account ist die versendete E-Mail zu sehen.

Der Link in der E-Mail führt auf eine gefälschte Webseite, welche unter Umständen mit den Echtdaten des Gastes arbeitet. Auch hier wird der Buchende nicht erkennen können, dass es ein Phishing-Angriff ist. Gibt er seine Daten zur Kreditkarte ein, wird ihm der offene Betrag vom Konto abgebucht. Das Geld ist weg! Den Schaden begleicht zunächst *booking.com*, wird aber versuchen, ihn auf das Hotel zu übertragen.

Was ist zu tun?

Es empfiehlt sich das Passwort zum *booking.com-Account* proaktiv zu ändern. Es sollte ein starkes Passwort mit mindestens 12 Zeichen (Groß- und Kleinbuchstaben + mind. 1 Zahl und 1 Sonderzeichen) verwendet werden. Für jeden Account der OTAs ist ein anderes Passwort zu verwenden!

Zu prüfen ist zudem, ob die Zwei-Faktoren-Authentifizierung aktiviert ist. Diese Prüfung sollte bei jedem OTA erfolgen, sofern dieser zusätzliche Schutz angeboten wird. Zu finden ist er meist bei den Einstellungen zum Passwort.

Was ist zu tun, wenn Sie einen Hack feststellen?

Trotz aller Vorsichtsmaßnahmen ist nie auszuschließen, dass Systeme gehackt werden. Sollte im Fall *booking.com* festgestellt werden, dass Phishing-Mails wie beschrieben an die Buchenden versendet wurden, ist schnell zu handeln.

1. Die Betroffenen sind unverzüglich über den *booking.com* Hotel-Account über den Angriff zu informieren und darauf hinzuweisen, dass keine persönlichen Daten insbesondere die Kreditkartendaten in das Formular eingegeben werden dürfen.
2. *booking.com* ist unverzüglich über den Angriff zu informieren. Sie werden im Nachgang ebenfalls eine Information an die Betroffenen versenden.
3. Der Vorfall ist als Datenpanne bzw. Datenschutzverstoß zu behandeln. Unverzüglich zu informieren sind die Hotelleitung und der Datenschutzbeauftragte. Der Vorfall ist meldepflichtig! Innerhalb von 72 Stunden nach Bekanntwerden des Hacks ist an die zuständige Aufsichtsbehörde für Datenschutz die Datenpanne zu melden.
4. Der Vorfall ist zu dokumentieren. Zu sammeln sind alle Beweise und Nachweise. Suchen sie auch die Phishing-Mail an das Hotel heraus.

Datenschutzbeauftragter DEHOGA Berlin | Andreas Thurmann | DataSolution LUD GmbH

www.datenschutzberater365.de