Betrug via BOOKING

Mit einer perfiden Masche attackieren Kriminelle seit Wochen Kunden des Buchungsportals. Dabei nutzen sie eine besondere Schwachstelle im System

VON BENEDIKT FUEST, KARSTEN SEIBEL UND DANIEL WETZEL

Die Nachricht des Hotels kommt per E-Mail. Und: Sie erscheint auch in der App des Buchungsportals Booking.com, direkt unter jener, in der das Hotel in Frankreich den Gast zuvor auf die Umleitung wegen einer Baustelle hingewiesen hatte. „Ich bin der Hauptverwalter des Hotels“, heißt es in der zweiten Nachricht. Die Bankkarte habe die Sicherheitsprüfung nicht bestanden. Der Kunde müsse seine Daten über den personalisierten Link von Booking.com aktualisieren, sonst gehe die Buchung verloren. „Innerhalb von zwölf Stunden“, heißt es, dann folgt ein rotes Ausrufezeichen.

Der Text enthält eigentlich alle Warnhinweise auf Betrug – leicht holpriges Englisch, übertriebene Hinweise auf Dringlichkeit und den Satz „Daten aktualisieren“. Doch die Nachricht kommt von einer vertrauenswürdigen Adresse: von Booking.com, der nicht nur in Deutschland dominanten Buchungsplattform für Hotels und Ferienwohnungen. Gegründet 1996 in Amsterdam, verfügbar in 43 Sprachen, können über das Portal 28 Millionen Unterkünfte weltweit gebucht werden.

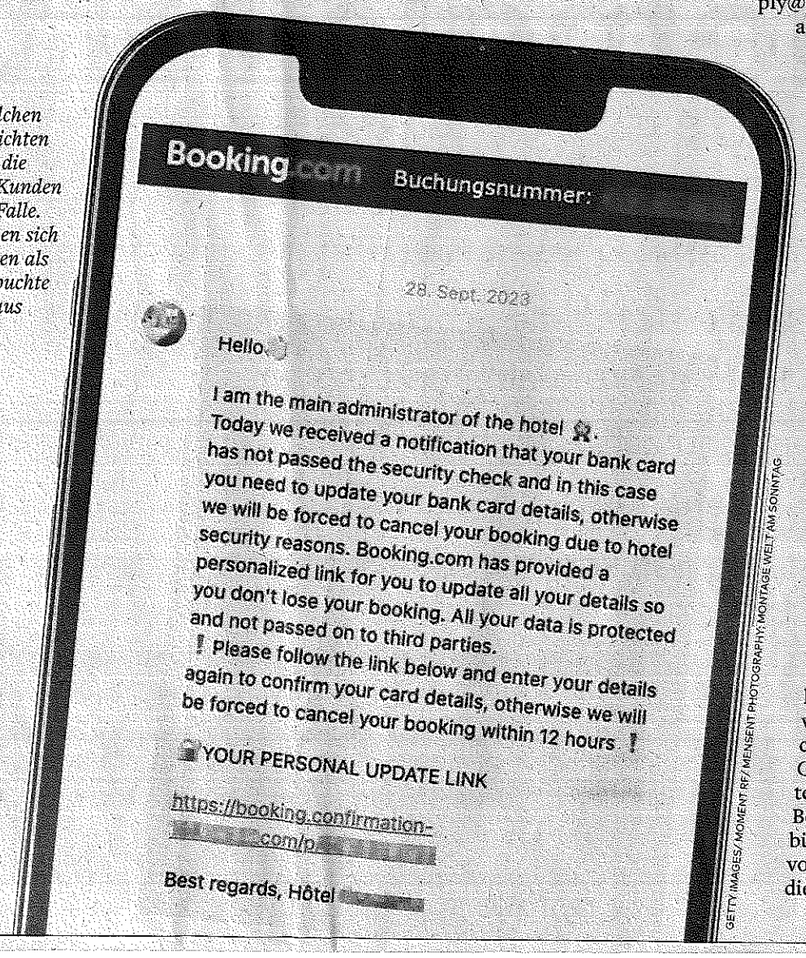
Wer auf den Link klickt und sorglos seine Daten eingibt, kommt spätestens ins Grübeln, nachdem die Kreditkarte belastet wurde – und als Empfänger nicht der Name des Hotels auftaucht. Ein Anruf bei dem gebuchten Hotel kommt zu spät. Das Geld ist weg. Diese perfide Masche läuft seit Wochen, wenn nicht sogar seit Monaten, genau lässt sich das nicht sagen. Booking.com gibt die Schuld den Hotels, die Hotels dem Buchungsportal. Zurück bleiben betrogene Kunden, die hoffen müssen, ihr Geld zurückzubekommen.

Markus Luthe, Hauptgeschäftsführer des Hotelverbands Deutschland, sieht in dem internen Kommunikationssystem von Booking.com schon länger ein Einfallstor für Phishing-Attacken und Fake-Buchungen. Die aktuelle Masche sei „besonders krass“. Die Betrüger würden gleichzeitig alle ausstehenden Buchungen eines Hotels, die zuvor über Booking.com hereinkamen, kontaktieren und zur nochmaligen Eingabe der Kreditkartendetails auffordern. „Dann stehen erst einmal für Stunden die Telefone an der Rezeption nicht mehr still, viele Gäste wollen wissen, was die Nachricht soll“, sagt Luthe. Andere würden die Buchung direkt stornieren, weil ihnen das Hotel nun suspekt vorkomme. Und dann würden sich auch noch jene melden, die bereits auf den Link gedrückt und gezahlt hätten.

Für Luthe ist das „ein multiples Sicherheits- und Kommunikationsversagen“ bei Booking. Das Unternehmen habe besondere Sorgfalts- und Abhilfepflichten. „Wer Nutzer und Hotelpartner zwingt, ausschließlich über das plattformeigene Extranet zu kommunizieren, der muss auch entsprechende Sicherheitsstandards gewährleisten“, sagt der Interessenvertreter der heimischen Hotelbranche. Zumal die Plattform genau mit der Betrugsgefahr rechtfertige, überhaupt Zugriff auf die Kommunikation zwischen Hotel und Gästen haben zu müssen.

Das Portal sieht den Grund dagegen bei den Hotels. „Einige unserer Unterkunftspartner wurden leider durch sehr überzeugende und ausgeklügelte Phishing-Taktiken dazu verleitet, auf Links in Phishing-E-Mails zu klicken oder Anhänge außerhalb unseres Systems herunterzuladen“, teilt die Firma mit. Dadurch lande Schadsoftware auf den Hotel-Computern und führe „zu einem nicht autorisierten Zugriff auf ihr Booking.com-Konto“. Die eigenen IT-Systeme seien aber nicht kompromittiert.

Dennoch befasse man sich intensiv mit dem Thema, versichert der Buchungsanbieter. Unter anderem setze man auf maschinelles Lernen, um verdächtige Aktivitäten schnell zu erkennen. Zudem arbeiteten „Teams unermüdlich daran, unsere Unterkunftspartner dabei zu unterstützen, ihre Systeme so schnell wie möglich zu sichern“. Zur Zahl der Angriffe und der Schadenshöhe will man sich nicht äußern.



Mit solchen Nachrichten locken die Täter Kunden in die Falle. Sie geben sich bei ihnen als das gebuchte Hotel aus

GETTY IMAGES/ MOMENT RF/ MENSENT PHOTOGRAPHY; MONTAGE WELT AM SONNTAG

Nicht nur in der Hotelbranche gehen Cyberkriminelle immer raffinierter vor. Die klassischen Phishing-Mails, die im E-Mail-Postfach landen, gibt es kaum noch. Betrugsmails werden von den großen Mail-Anbietern wie Googlemail und GMX sehr viel besser erkannt und direkt ins Spam-Postfach sortiert. Deshalb suchen Betrüger nach immer neuen Möglichkeiten, an den Filtern vorbei zu ihren Opfern gelangen. Im Fall des Booking.com-Betrugs haben sie nicht nur Zugang zum Kommunikationskanal der App gefunden. Die zusätzliche Mail kommt von der Adresse noreply@booking.com, von der auch alle regulären E-Mails rund um Hotelbuchungen, Reservierungsbestätigungen und Werbemails des Hotelportals stammen. Dafür müssen die Kriminellen keinen Booking.com-Server hacken. Viel einfacher ist es, die meist einfache IT-Infrastruktur kleiner Hotels anzugreifen.

Was eigentlich nicht möglich sein sollte, ist, eine Zahlungsabwicklung anzustoßen. Denn dafür hat Booking.com ein eigenes System aufgebaut: Die Kunden können ihre Kreditkartendaten in dem Portal hinterlegen, das Portal wickelt die Zahlung sicher ab und gibt das Geld an die Hotels weiter. Doch dabei behält Booking.com eine Gebühr ein. Deswegen bevorzugen einige Hotels, die Zahlung selbst abzuwickeln, mit allen Risiken, die darin für den Gast liegen. Daher dürften viele der Betrugsopfer nicht überrascht sein, wenn plötzlich das Hotel nach Zahlungsinformationen fragt. Sie tippen auf den Link.

Dieser lautet beispielsweise https://booking.confirmation-123456.com/p/123456. Er leitet auf den ersten Blick zu einem Server des Buchungsportals. Was viele unbedarfte Nutzer nicht wissen: Die echte Domain ist nur der Teil der Adresse unmittelbar vor der Zeichenfolge „.com“. Der Server hat in dem Fall also nichts mit Booking.com gemein, auch wenn die Adresse mit dem Namen des Portals beginnt. Die Internetseite dahinter sieht vertrauenswürdig aus, ganz im blauen Seitendesign des Portals. Gibt der verwirrte Hotelgast hier nun noch einmal seine Zahlungsdaten ein, hat der Täter das Geld auf seinem Konto.

Ist der Betrug erkannt, sollten Geschädigte sofort ihre Bank informieren und die Karte sperren lassen, rät Alina Menold von der Verbraucherzentrale Niedersachsen. Falls über Paypal bezahlt wurde, könnten sie den Käuferschutz aktivieren. Wichtig sei immer, die Nachrichten und Belege im Zusammenhang mit der Buchung zu dokumentieren, also entsprechende Screenshots zu machen. Viel Hoffnung kann sie Verbrauchern nicht machen. „Leider ist das Geld meist verloren“, sagt Menold.

Booking.com selbst versichert auf Anfrage, betroffenen Kunden zu helfen – ohne näher auf das Wie einzugehen. WELT AM SONNTAG liegt ein Schreiben vor, in dem sich das Unternehmen für die Unannehmlichkeiten entschuldigte. „Unsere Gäste sollen das beste Reiseerlebnis haben“, heißt es darin. Deshalb möchte man ein Wallet-Guthaben in Höhe des Schadens zurückerstatten. Was dann auch geschah. In welchen Fällen so verfahren wird, dazu will sich das Unternehmen nicht äußern. Vermeintliche Opfer sollten sich mit dem Kundenservice in Verbindung setzen, teilt es lediglich mit, damit dieser den „individuellen Fall prüfen und sie unterstützen“ könne.

ANZEIGE