feratelInfoMail

Sicherheitsforscher warnen aktuell vor einer **verstärkten Angriffswelle auf die europäische Hotelbranche**. Dabei kommen insbesondere Phishing- und Social-Engineering-Methoden zum Einsatz, um **Mitarbeitende von Hotels** zur Preisgabe von Zugangsdaten oder zur Ausführung schädlicher Aktionen zu bewegen (Details siehe weiterführende Informationen unten).

In diesem Zusammenhang erreichen uns bereits Rückmeldungen von Betrieben, die aufgrund verdächtiger Nachrichten einen möglichen Sicherheitsvorfall der Buchungsplattform vermuten.

Als technischer Dienstleister möchten wir klarstellen:

Nach aktueller Prüfung liegen **keine Hinweise auf einen technischen Angriff, eine Sicherheitslücke oder einen Datenabfluss innerhalb der Deskline Buchungsplattform** vor. Die Systeme werden laufend überwacht und entsprechen den geltenden Sicherheitsstandards.

Die geschilderten Fälle entsprechen vielmehr einem **externen Phishing- bzw. Malware-Szenario**, das derzeit branchenweit auftritt. Die Angriffe erfolgen **außerhalb der Buchungsplattform** und setzen in der Regel voraus, dass Zugangsdaten über gefälschte E-Mails oder Webseiten eingegeben wurden.

Typisches Resultat dieser Angriffe ist, dass gebuchte Gäste anschließend eine täuschend echt gestaltete Zahlungsaufforderung erhalten.
Die dafür verwendeten Buchungsinformationen werden dabei **nicht aus der Buchungsplattform**, sondern aus kompromittierten Systemen des jeweiligen Betriebs ausgelesen – meist aus **E-Mail-Konten an lokal genutzten Arbeitsplätzen**, auf die sich Angreifer nach erfolgreichem Phishing Zugriff verschafft haben.

Ergänzend möchten wir darauf hinweisen, dass **auch Hotelverbände sowie Anbieter von Hotelsoftware ihre Kunden bereits aktiv über diese Angriffsmuster informieren und den typischen Ablauf solcher Phishing-Angriffe nachvollziehbar darstellen**, um das Bewusstsein und die Aufmerksamkeit in den Betrieben weiter zu stärken (siehe weiterführenden Link unten).

Wir empfehlen Hotels weiterhin:

- Zugangsdaten niemals über E-Mail-Links oder externe Seiten einzugeben
- sich ausschließlich über bekannte, offizielle Zugangswege anzumelden
- verdächtige Nachrichten nicht zu beantworten und zu löschen

Weiterführende Informationen:

- Erläuterung typischer Phishing-Abläufe im Hotelumfeld (lesenswerte Information eines Hotelsoftware-Anbieters): https://blog.easybooking.eu/phishing-hotellerie-cyberangriffe/
- Warnung von Sicherheitsforschern vor aktuellen Angriffen auf Hotels: https://www.it-daily.net/shortnews/malware-angriffe-europaeische-hotels
- Warnungen von Hotelverbänden: https://www.oehv.at/recht-service/warnungen/ https://www.hotellerie.de/news/warnungen