مجموعة Flight Centre Travel Group تعلن احتمال الوصول إلى بيانات عملاء عبر نظام حجز تابع لجهة خارجية



أعلنت Flight Centre Travel Group أن جهات مجهولة ربما وصلت إلى سجلات عملاء في نظام حجز إقامة تديره جهة خارجية، وأغلبها أسماء، مع بيانات جوازات وصحة محدودة في حالات نادرة. ولم يُرصد وصول إلى بيانات الدفع حتى الآن.

- يتعلق الحادث بنشاط غير معتاد في نظام حجز إقامة تديره جهة خارجية تستخدمه علامة Flight Centre وTravel Associates وCruiseabout وبعض الوكلاء المستقلين.
- تحتوي معظم السجلات التي جرى الوصول إليها على أسماء فقط، وبعضها يضم معلومات سفر أساسية؛ وتشمل نسبة ضئيلة جدًا بيانات جواز محدودة أو وسائل اتصال أو تواريخ ميلاد، وفي حالات نادرة معلومات صحية أو عن الحركة.
- لم يُرصد حتى الآن أي وصول إلى بطاقات الائتمان أو بيانات الدفع أو الحسابات المصرفية.
- تفيد الشركة بأن حجوزات الطيران وحجوزات سفر الشركات غير متأثرة.

- تعمل الشركة مع المورّد ومع Mandiant، وغيّرت مفاتيح المصادقة وبيانات الاعتماد، وتُبلغ الجهات المختصة.

أبلغت مجموعة Flight Centre Travel Group (FLT)، ومقرها بريسبان، بورصة الأوراق المالية الأسترالية بأنها تحقق في نشاط غير معتاد داخل نظام تابع لجهة خارجية يُستخدم لحجز الإقامة، وتعتمد عليه علامة Flight Centre وTravel Associates وCruiseabout وبعض الوكلاء المستقلين.

ما هو معروف

تعتقد الشركة أن عددًا كبيرًا من سجلات العملاء في النظام المتأثر ربما جرى الوصول إليه، لكن لم يتضح بعد كم منها جرى استخراجه فعليًا. وتشير المراجعة الأولية إلى أن أغلب السجلات تضم أسماء فقط، وأحيانًا مع معلومات سفر أساسية. وقد تشمل نسبة ضئيلة جدًا بيانات جواز سفر محدودة أو عناوين بريد إلكتروني أو أرقام هاتف أو تواريخ ميلاد، وفي حالات نادرة معلومات صحية أو عن القدرة على الحركة.

ولم ترصد الشركة حتى الآن أي وصول إلى بطاقات الائتمان أو بيانات الدفع أو الحسابات المصرفية. وتفيد بأن حجوزات الطيران وحجوزات سفر الشركات تتم عبر أنظمة أخرى ولم تتأثر.

الاستجابة والسياق الأوسع

فعّلت FLT خطة الاستجابة للحوادث، وعملت مع الجهة الخارجية على احتواء النشاط، وغيّرت مفاتيح المصادقة وبيانات الاعتماد، وشددت المراقبة، وتُبلغ الجهات المختصة. وتعمل مع المورّد ومع Mandiant لتحديد نطاق الحادث. وتنصح العملاء بالحذر من أي رسائل أو مكالمات غير متوقعة بشأن الحجوزات، وعدم فتح الروابط أو المرفقات أو مشاركة بيانات شخصية أو مالية.

وتشير المصدر إلى أن الحادث يأتي بعد وقائع أخرى مرتبطة بأنظمة الحجز، منها تحذير Booking.com في أبريل، واختراق لدى RMS Cloud مزوّد برمجيات الإقامة، تلاه تلقي نزلاء رسائل تصيّد.

الأهمية للمؤسسات في المملكة

يبيّن الحادث كيف يمكن لمنصة مورّد واحدة أن تكشف بيانات تخص عدة علامات تجارية. وعلى المؤسسات التي تعتمد على منصات السفر أو الضيافة في حجوزات الموظفين أو العملاء أو الوفود أن تراجع ما تحتفظ به هذه الجهات من بيانات شخصية، ومدى سرعة إبلاغها عند وقوع حادث.

ما يجب فعله الآن

1. حصر منصات حجز السفر والإقامة التابعة لجهات خارجية المستخدمة لسفر الموظفين والوفود، وتحديد البيانات الشخصية التي تحتفظ بها كل منصة ومنها بيانات الجوازات.
2. مطالبة هذه الجهات بتأكيد كتابي بشأن تأثرها من عدمه وآلية إبلاغكم بالحوادث.
3. تذكير الموظفين المسافرين والتنفيذيين بأن الرسائل غير المتوقعة عن الحجوزات قد تكون تصيّدًا، والتحقق منها عبر قنوات معروفة.
4. التأكد من أن عقود الموردين تُلزم بالإبلاغ الفوري عن الاختراقات وتدعم الالتزامات الواردة في نظام

حماية البيانات الشخصية (PDPL) بشأن الإبلاغ عن الحوادث.

5. مراجعة إجراءات تدوير بيانات الاعتماد ومفاتيح الربط مع الموردين لضمان تنفيذها بسرعة عند وقوع حادث.