Fandango تُبلغ عملاءها بسرقة بيانات بطاقات الدفع من صفحات الدفع



تُبلغ شركة Fandango Media عملاءها بحادث اختراق كشف بيانات بطاقات الدفع المُدخلة في صفحات الدفع لديها. ولا يتضمن المقتطف المتاح تفاصيل إضافية.

- تُخطر Fandango Media، وهي شركة لبيع التذاكر، عملاءها بوقوع حادث اختراق بيانات.
- البيانات المكشوفة هي تفاصيل بطاقات الدفع المُدخلة في صفحات الدفع.
- النص المتاح من المصدر مقتطع، لذا لا يمكن تأكيد حجم الحادث أو توقيته أو أسلوبه.

ما الذي أُعلن

بدأت Fandango Media، وهي شركة لبيع التذاكر، إخطار عملائها بحادث اختراق بيانات. وبحسب التقرير، حصل المهاجمون على بيانات بطاقات الدفع التي أدخلها العملاء في صفحات الدفع الخاصة بالشركة.

ما لم يتضح بعد

النص المتاح لنا مقتطع بعد الأسطر الأولى، ولا يذكر عدد المتضررين، ولا توقيت النشاط، ولا كيفية وصول المهاجمين، ولا ما اتخذته الشركة من إجراءات. لذلك لم نورد أيًا من هذه النقاط، وننصح القراء بالرجوع إلى التقرير الأصلي وإشعار الشركة.

الأهمية للجهات في المملكة

يذكّر الحادث بأن صفحات الدفع هدف مباشر: فالبيانات التي يدخلها العميل عند إتمام الشراء قد تتعرض للكشف حتى لو كانت الأنظمة الخلفية محمية جيدًا. وعلى الجهات التي تقبل المدفوعات الإلكترونية، أو تعتمد على نصوص برمجية ومكونات دفع من أطراف ثالثة في هذه الصفحات، أن تعدّ ذلك دافعًا لمراجعة سلامة مسارات الدفع لديها ومراقبتها. فالمراجعة الهادئة المبنية على الأدلة أجدى من ردة الفعل المتسرعة.

ما يجب فعله الآن

1. حصر جميع النصوص البرمجية ومكونات الأطراف الثالثة المحمّلة في صفحات الدفع.
2. تفعيل اكتشاف التغييرات والتنبيه عليها في محتوى صفحات الدفع ونصوصها البرمجية.
3. التأكد من فاعلية ضوابط PCI DSS الخاصة بصفحات الدفع وتوثيق أدلتها.
4. التحقق من أن خطة الاستجابة للحوادث تغطي كشف بيانات البطاقات، بما في ذلك التزامات الإبلاغ وفق نظام حماية البيانات الشخصية (PDPL) والجهات التنظيمية القطاعية.
5. مراجعة التقرير الأصلي وإشعار الشركة قبل استخلاص أي استنتاجات عن الأثر.