اختراق لدى مورّد برمجيات يكشف بيانات المستفيدين في أكثر من 40 اتحاد ائتمان أيرلندي



استغل مهاجمون ثغرة لدى المورّد Wellington IT وطالوا بيانات المستفيدين لأعضاء أكثر من 40 اتحاد ائتمان أيرلندي. أُغلقت الثغرة في 6 أكتوبر، ولم يُبلَّغ العملاء إلا في 16 نوفمبر.

- تلقّت هيئة حماية البيانات الأيرلندية أكثر من 40 إشعار خرق من اتحادات ائتمان تعتمد على Wellington IT كمعالج للبيانات.
- يفيد المسؤولون بأن الأثر اقتصر على بيانات المستفيدين المخزنة في تطبيقات الخدمات المصرفية عبر الجوال التي يشغّلها Wellington IT، ولم يطل الأعضاء الذين لا يستخدمونها.
- أغلقت Wellington IT الثغرة في 6 أكتوبر، لكن تحقيقها الأولي لم يحدد وقوع خرق للبيانات.
- أُبلغت الاتحادات المتضررة في 16 نوفمبر، وهو تأخير وصفه وزير الدولة الأيرلندي بأنه غير مقبول.
- لا توجد حتى الآن أدلة على الوصول إلى الأموال أو وقوع احتيال.

طال مهاجمون بيانات دفع تخص أعضاء أكثر من 40 اتحاد ائتمان أيرلنديًا بعد استغلال ثغرة في أنظمة Wellington IT، وهي شركة برمجيات مقرها بلفاست. وأكدت هيئة حماية البيانات الأيرلندية أنها تلقّت أكثر من 40 إشعار خرق من اتحادات تستخدم الشركة معالجًا للبيانات.

ما هو معروف

وقع الهجوم في أوائل أكتوبر بحسب الرئيس التنفيذي للرابطة الأيرلندية لاتحادات الائتمان. وتفيد Wellington IT بأنها أغلقت الثغرة في 6 أكتوبر، لكن تحقيقها الأول لم يخلص إلى وقوع خرق لحماية البيانات. ولم تُبلَّغ الاتحادات إلا في 16 نوفمبر.

وقال وزير الدولة الأيرلندي روبرت تروي إن الحادثة اقتصرت على بيانات المستفيدين المخزنة لدى الأعضاء الذين يستخدمون تطبيقات الخدمات المصرفية عبر الجوال التي تشغّلها Wellington IT. وأفاد هو والمركز الوطني للأمن السيبراني في أيرلندا بعدم وجود دليل حاليًا على الوصول إلى الأموال أو وقوع احتيال. واستعانت الشركة بخبراء خارجيين لتحديد العدد الدقيق للحسابات والمستخدمين المتأثرين.

وتمتد الحادثة عبر ولايتين قضائيتين، إذ لم يتلقَّ مكتب مفوض المعلومات في المملكة المتحدة بلاغًا من الشركة، لكنه بدأ يستقبل بلاغات من اتحادات الائتمان، ما يشير إلى احتمال تأثر أعضاء في المملكة المتحدة.

الأهمية للجهات المنظَّمة

تبيّن الحالة أن ثغرة أُصلحت لدى المورّد قد تتحول إلى خرق واجب الإبلاغ لدى عملائه، وأن الفجوة بين المعالجة التقنية وتقييم الخرق تؤخر الإشعار. وبقي العملاء هم الجهات المسؤولة رغم وجود البيانات لدى المعالج.

وتواجه المؤسسات السعودية التي تعتمد على معالجين خارجيين لخدمات الجوال أو المدفوعات الاعتماد نفسه.

ما يجب فعله الآن

1. راجع عقود المعالجين والموردين لاشتراط الإبلاغ الفوري عن الحوادث المشتبه بها وليس المؤكدة فقط.
2. اطلب من الموردين الحرجين بيان نطاق أي ثغرة جرى إصلاحها والأدلة التي استُندت إليها في استبعاد تعرض البيانات.
3. حدّد البيانات التي تقع ضمن تطبيقات الجوال والمدفوعات التي يشغّلها الموردون، مثل بيانات المستفيدين.
4. اختبر إجراءات الاستجابة لديك لاتخاذ قرار الإبلاغ إلى سدايا أو البنك المركزي السعودي أو الهيئة الوطنية للأمن السيبراني ضمن المدد المطلوبة بموجب نظام حماية البيانات الشخصية والأطر ذات الصلة.
5. أدرج سيناريوهات اختراق الموردين في مراجعات مخاطر الأطراف الثالثة وتمارين المحاكاة.