اختراق لدى مزوّد خدمة خارجي يكشف بيانات عملاء Chase



حذّرت J.P. Morgan Chase من اختراق بيانات إثر هجوم سيبراني على مزوّد خدمة خارجي، كشف معلومات شخصية للعملاء وبيانات تسويقية. وتذكر العناوين أيضاً عملاء Visa وMastercard.

- أعلنت Chase عن اختراق بيانات منشؤه مزوّد خدمة خارجي.
- شملت البيانات المكشوفة معلومات شخصية للعملاء وبيانات تسويقية.
- يربط عنوان المصدر الحادثة أيضاً ببيانات عملاء Visa وMastercard.
- تذكّر الحادثة بأن أمن الموردين يؤثر مباشرة في مخاطر بيانات المؤسسة.

ما الذي أُعلن

حذّرت J.P. Morgan Chase من تعرّضها لاختراق بيانات. وبحسب التقرير، كان السبب هجوماً سيبرانياً على مزوّد

خدمة خارجي وليس على أنظمة البنك نفسها. وتشمل المعلومات المكشوفة بيانات شخصية للعملاء وبيانات تسويقية.

ويشير عنوان التقرير كذلك إلى معلومات عملاء Visa وMastercard. أما المقتطف المتاح لنا فلا يتضمن تفاصيل إضافية، لذا ينبغي التحقق من عدد المتأثرين وحقول البيانات المحددة وهوية المزوّد والجدول الزمني من التقرير الكامل والإشعارات الرسمية.

لماذا يهم المؤسسات في المملكة

توضح الحادثة نمطاً معروفاً: قد تملك المؤسسة ضوابط داخلية قوية ومع ذلك تنكشف بيانات عملائها عبر مورّد يعالجها نيابة عنها. وغالباً ما تكون البيانات الشخصية والتسويقية المشاركة مع الموردين أقل إحكاماً في الحوكمة من بيانات الأنظمة المصرفية الأساسية، رغم أنها قد تحمل الالتزامات الخصوصية نفسها.

وبالنسبة للجهات الخاضعة لإشراف البنك المركزي السعودي (ساما) والهيئة الوطنية للأمن السيبراني ولنظام حماية البيانات الشخصية، تدخل الجهات المعالِجة من الأطراف الثالثة ضمن نطاق المساءلة. ولذلك تصبح قوائم الموردين والمتطلبات التعاقدية الأمنية وشروط الإبلاغ عن الحوادث مسائل عملية لا إجراءات شكلية.

النهج المقترح

لا يتطلب الأمر إجراءً فنياً محدداً لغياب أي مؤشرات اختراق في التقرير. والخطوة المناسبة هي استثمار هذه الحادثة لاختبار ترتيبات الموردين لديكم، بدءاً بمن يحتفظ ببيانات شخصية أو تسويقية للعملاء.

ما يجب فعله الآن

1. حدّثوا قائمة مزوّدي الخدمة الذين يعالجون بيانات العملاء الشخصية أو التسويقية.
2. راجعوا العقود للتأكد من وجود متطلبات أمنية ومهل واضحة للإبلاغ عن الحوادث.
3. تحققوا من البيانات التي يحتفظ بها كل مورّد واحذفوا ما لم يعد مطلوباً.
4. تأكدوا من أن خطة الاستجابة للحوادث تغطي الاختراق الذي ينشأ لدى مورّد، بما في ذلك خطوات الإشعار وفق نظام حماية البيانات الشخصية.
5. اطلبوا من الموردين عالي المخاطر أدلة ضمان حديثة مثل تقارير التدقيق أو نتائج الاختبار.