بنك الدولة الهندي يؤكد تسرب بيانات عملاء ظهرت على الويب المظلم



أعلن بنك الدولة الهندي أن 3,897 سجلًا لعملاء تتضمن بيانات شخصية ضمن نحو 375,000 سجل متاح على الويب المظلم، ولم يتضح بعد مصدر البيانات.

- رُصد 3,897 سجلًا لعملاء تتضمن بيانات شخصية ضمن مجموعة من نحو 375,000 سجل على الويب المظلم.
- لا يعرف البنك حتى الآن مصدر البيانات.
- جاء الإفصاح في إشعار لبورصة الأوراق المالية بتاريخ 21 أكتوبر.
- وصف الإشعار الحادثة بأنها فقدان لبعض البيانات.
- البنك مملوك للدولة وهو أكبر بنوك الهند.

ما الذي أُعلن

أكد بنك الدولة الهندي، أكبر بنوك الهند والمملوك للدولة، ظهور بيانات عملاء على الويب المظلم. وذكر في إشعار لبورصة الأوراق المالية بتاريخ 21 أكتوبر أنه تعرض لحادثة تتعلق بفقدان بعض البيانات.

وحدد البنك 3,897 سجلًا لعملاء تتضمن معلومات شخصية ضمن مجموعة أكبر تضم نحو 375,000 سجل متاحة على الويب المظلم.

ما لا يزال مجهولًا

وفق التقرير، لا يعرف البنك حتى الآن مصدر البيانات. ولا يوضح المصدر كيفية الحصول على السجلات، ولا طبيعة الحقول التي تحويها بخلاف المعلومات الشخصية، ولا ما إذا كانت بقية السجلات في المجموعة تخص البنك.

وإلى أن يتضح المصدر، يصعب الجزم بأن الأمر اختراق لأنظمة البنك نفسه أو لطرف ثالث أو تجميع لبيانات قديمة. وهذا الغموض بحد ذاته درس مفيد لبقية المؤسسات.

أهمية الحادثة للمؤسسات السعودية

تبين الحالة أن التسرب قد يُكتشف من الخارج قبل فهم السبب الجذري. ينبغي للجهات المنظمة في المملكة أن تكون جاهزة لتقييم حادثة كهذه والإبلاغ عنها والتحقيق ما زال مفتوحاً، وأن تعرف أي بيانات للعملاء لدى أي معالج أو شريك.

وهي فرصة مناسبة لاختبار رصد الويب المظلم ودقة جرد البيانات ومسار القرار لإشعار الجهات التنظيمية والأفراد المتأثرين.

ما يجب فعله الآن

1. تأكد من أن رصد الويب المظلم والتسريبات يغطي علامتكم التجارية وعينات من بيانات العملاء وأهم الأطراف الثالثة.
2. تحقق من أن جرد البيانات يبين مواضع حفظ البيانات الشخصية للعملاء، بما فيها لدى المعالجين والموردين.
3. تدرّبوا على سيناريو ظهور بيانات مسربة مجهولة المصدر، بما يشمل الفرز وتحديد المصدر.
4. راجعوا مسار الإبلاغ عن الاختراقات وفق نظام حماية البيانات الشخصية ومدد إشعار الجهة التنظيمية والعملاء المتأثرين.
5. تأكدوا من ربط التزامات الإبلاغ أمام البنك المركزي السعودي والهيئة الوطنية للأمن السيبراني بخطة الاستجابة للحوادث.