ولاية كولورادو توقف تطبيق myColorado بعد هجوم سيبراني وسرقة محتملة لبيانات نحو 150 ألف شخص



أوقف مكتب تقنية المعلومات في كولورادو تطبيق myColorado بعد اكتشاف اختراق في 18 نوفمبر، ويرجَّح سرقة بيانات تخص نحو 150 ألف مستخدم من أصل 2.1 مليون.

- اكتُشف الاختراق مساء 18 نوفمبر، فأوقفت الولاية التطبيق وبدأت التحقيق.
- للتطبيق 2.1 مليون مستخدم، ويرجَّح أن بيانات نحو 150 ألف شخص سُرقت.
- لم يوضح المحققون نوع البيانات المسروقة.
- ظل التطبيق متوقفًا حتى ظهر الثلاثاء، ويمكن للسكان استخدام مواقع الجهات الحكومية، مع نصحهم بحمل هوياتهم الورقية أثناء السفر.
- يشير التقرير إلى موجة أوسع من الهجمات على جهات حكومية محلية في الولايات المتحدة، منها هجمات فدية.

ما الذي حدث

أعلن مكتب تقنية المعلومات التابع لحاكم ولاية كولورادو (OIT) أنه اكتشف مساء 18 نوفمبر اختراق مهاجمين لتطبيق myColorado، الذي يستخدمه السكان للهوية الرقمية وحفظ الوثائق والوصول إلى الخدمات الحكومية. وأوقف المكتب التطبيق وبدأ التحقيق، وظل التطبيق غير متاح حتى ظهر الثلاثاء.

وذكرت الولاية أن للتطبيق 2.1 مليون مستخدم، وأن الهجوم يرجَّح أنه شمل سرقة بيانات تخص نحو 150 ألف شخص. ورفض المحققون الإفصاح عن نوع البيانات المسروقة. وقالت المديرة التنفيذية للمكتب إن حماية بيانات المستخدمين أولوية، وإن الأنظمة ستعود بعد استعادة الأمان.

الأثر والسياق الأوسع

نصحت الولاية السكان بحمل هوياتهم الورقية عند السفر في عطلة عيد الشكر، ولا يزال بإمكانهم الوصول إلى الخدمات عبر مواقع الجهات الحكومية. وسبق أن تعرضت الولاية لهجمات استهدفت إدارة التعليم العالي وهجمات فدية على بلديات أصغر.

ويورد التقرير حوادث حديثة أخرى في جهات عامة أمريكية، منها هجوم فدية على مكتبة كوينز العامة في نيويورك، وهجوم على مكتب شرطة مقاطعة في ميسيسيبي، وهجوم أخرج الهيئة التشريعية في فرجينيا الغربية عن الخدمة.

لماذا يهم المؤسسات المنظمة

تبين الحالة أن منصة واحدة للهوية والخدمات الرقمية قد تصبح نقطة ضعف للبيانات واستمرارية الخدمة معًا. ويمثل اللجوء إلى مواقع الجهات والهويات الورقية مثالاً على التخطيط لفقدان القناة الرقمية. ولم تُعلن تفاصيل البيانات المسروقة، لذا ينبغي انتظار مزيد من المعلومات الرسمية قبل تقدير حجم التعرض.

ما يجب فعله الآن

1. راجعوا ما إذا كان أي تطبيق للهوية الرقمية أو لخدمة العملاء يمثل القناة الوحيدة لخدمات حرجة، وحددوا قناة بديلة مجرَّبة.
2. تأكدوا أن خطط الاستجابة للحوادث تشمل إيقاف تطبيق عام والتواصل مع العملاء وقرار موعد إعادة التشغيل.
3. طابقوا إجراءات الإبلاغ عن الاختراقات مع متطلبات نظام حماية البيانات الشخصية (PDPL) وتواصلوا مع سدايا والجهة التنظيمية القطاعية عند الاقتضاء.
4. احصروا البيانات الشخصية المخزنة في تطبيقات العملاء ومستودعات الوثائق، وتحققوا من ضوابط الوصول والسجلات والتشفير.
5. اختبروا استمرارية الأعمال عند فقدان خدمة رقمية وفق متطلبات استمرارية الأعمال لدى البنك المركزي السعودي (SAMA BCM) أو الضوابط الأساسية للأمن السيبراني (NCA ECC).