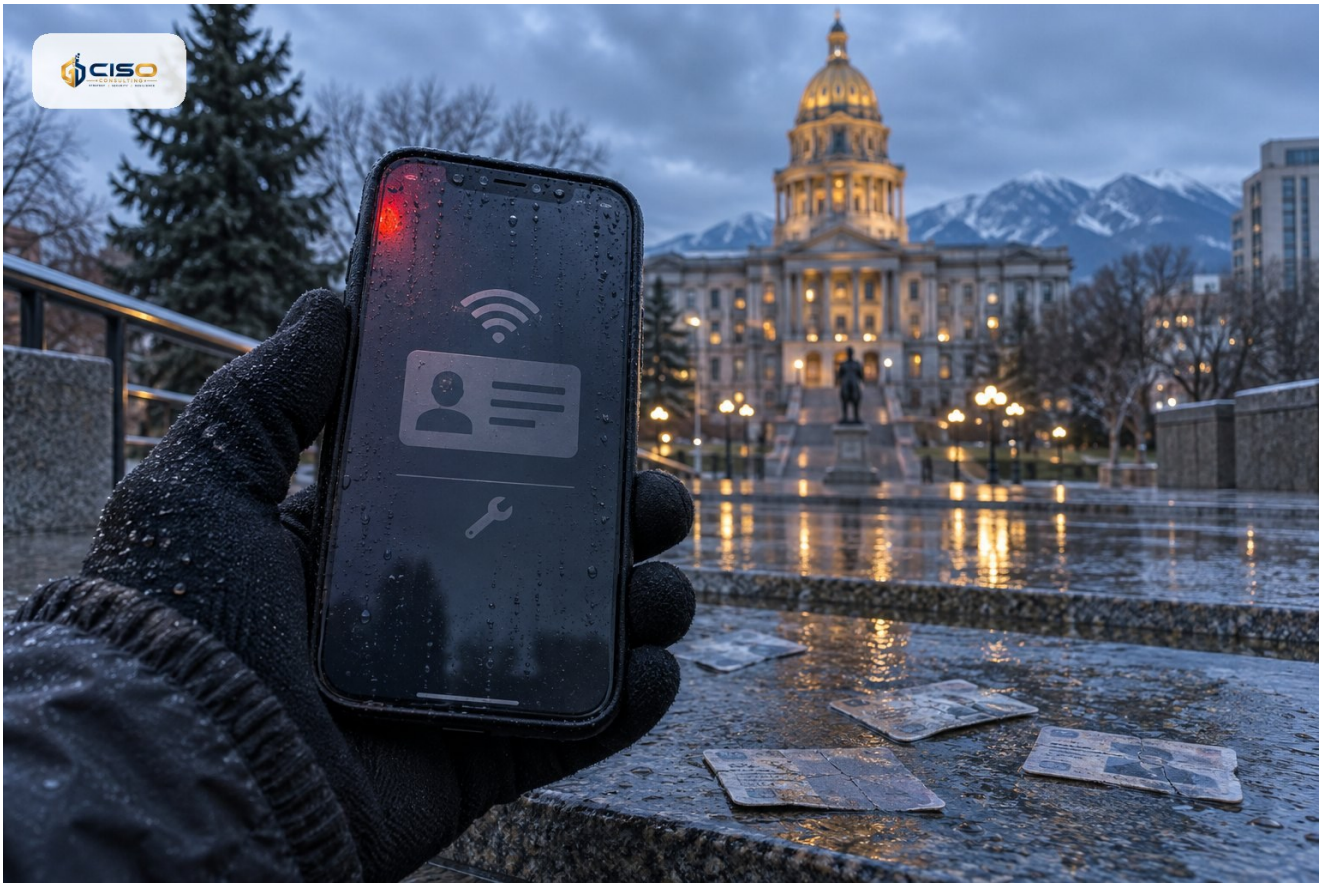
اختراق تطبيق myColorado في ولاية كولورادو قد يطال نحو 100 ألف شخص



أعلن مكتب تقنية المعلومات في كولورادو أن مهاجمين وصلوا إلى وثائق هوية رفعها مستخدمو تطبيق myColorado. قد يتأثر نحو 100 ألف شخص، ولم تُمسّ بيانات الدفع، والتطبيق متوقف.

- طال الوصول غير المصرح به قسم «myCards and Documents» في تطبيق myColorado الذي يبلغ عدد مستخدميه نحو 2.1 مليون.
- شملت الملفات المكشوفة ملفات PDF وصور هويات حكومية وتسجيلات مركبات وبطاقات تأمين.
- قد يتأثر نحو 100 ألف شخص، وقد يُعدَّل التقدير مع مطابقة الوثائق بالمستخدمين.
- لم يُطَّلع على أي معلومات دفع.
- كُشف الحادث عبر أنظمة الكشف الآلي عن التهديدات في بيئة AWS، ومن المتوقع بدء الإشعارات في 27 نوفمبر.

أعلن مكتب تقنية المعلومات التابع لحاكم ولاية كولورادو (OIT) عن اختراق طال وثائق رفعها السكان إلى تطبيق myColorado، وهو التطبيق الرسمي للولاية للهوية الرقمية والخدمات الحكومية وتخزين المستندات، ويبلغ عدد مستخدميه نحو 2.1 مليون.

ما الذي حدث

أوقف المكتب التطبيق بعد رصد وصول غير مصرح به إلى بيانات المنصة، وبدأ الاستجابة للحادث والتحقيق فيه. وذكر أن الحادث كُشف عندما فعّل المهاجمون أنظمة الكشف الآلي عن التهديدات المنشورة في بيئة Amazon Web Services (AWS) التابعة له.

وتبيّن من التحقيق أن المهاجمين وصلوا إلى قسم «myCards and Documents» الذي يضم ملفات PDF وصور هويات حكومية وتسجيلات مركبات وبطاقات تأمين رفعها المستخدمون. وقد يكون نحو 100 ألف شخص متأثرين، ولم يُطَّلع على أي معلومات دفع.

الوضع الحالي

يعمل الفريق على مطابقة الوثائق التي جرى الوصول إليها بالمستخدمين، وأفاد المكتب بأنه سيعدّل التقدير مع تقدم هذا العمل. ما زال التطبيق متوقفاً دون إعلان موعد لاستعادته، ومن المتوقع بدء إرسال الإشعارات المباشرة للمتأثرين في 27 نوفمبر. وأوضح مدير المعلومات في الولاية أن الأولوية لحماية المستخدمين وإشعار المعنيين وإعادة التطبيق مع تعزيزات أمنية.

أهمية الحادث للمؤسسات في المملكة

يبيّن الحادث أن الوثائق التعريفية التي يرفعها المستخدمون إلى خدمة سحابية تمثل مخاطر مركّزة، وأن الكشف الآلي قد يُظهر الاختراق. وعلى الجهات التي تجمع نسخاً من الهويات الوطنية أو وثائق المركبات والتأمين مراجعة طريقة تخزينها ومراقبتها ومدة الاحتفاظ بها.

ما يجب فعله الآن

1. حصر أماكن تخزين صور وثائق الهوية للعملاء أو الموظفين، بما فيها التخزين السحابي، وتحديد من يملك صلاحية الوصول إليها.
2. تطبيق التشفير وأقل الصلاحيات وحدود الاحتفاظ على وثائق الهوية المخزنة.
3. التأكد من أن الكشف عن التهديدات في البيئة السحابية يغطي مخازن الوثائق المرفوعة وأن التنبيهات تصل إلى فريق استجابة فعّال.
4. اختبار إجراءات الاستجابة للحوادث والإبلاغ عن الاختراقات وفق نظام حماية البيانات الشخصية (PDPL)، بما في ذلك تحديد الأفراد المتأثرين من الملفات التي جرى الوصول إليها.
5. إعداد نموذج للتواصل مع العملاء وخطة لإيقاف الخدمة وإعادتها بأمان.