Turnitin تحقق في هجوم سيبراني استهدف أنظمتها المواجهة للعملاء



أعلنت Turnitin رصد نشاط غير مصرح به في بعض أنظمتها المواجهة للعملاء، وتؤكد أن خدماتها تعمل. ولم تذكر هل جرى الوصول إلى بيانات أو عدد العملاء المتأثرين.

- أبلغت Turnitin، التابعة لشركة Advance Publications، في رسالة بتاريخ 23 نوفمبر عن نشاط غير مصرح به في بعض أنظمتها المواجهة للعملاء.
- فعّلت الشركة خطة الاستجابة للحوادث، وأبلغت الجهات المعنية، واستعانت بخبراء سيبرانيين خارجيين.
- تفيد الشركة بأن هذه الأنظمة لا تجمع وثائق الهوية الحكومية ولا المعلومات المالية للمؤسسات.
- لم توضح الشركة أي الأنظمة اختُرقت، ولا هل جرى الوصول إلى بيانات، ولا عدد العملاء المتأثرين.
- ذكرت جامعة كولورادو بولدر أنه لا مؤشر على تعرض بياناتها، وأضافت مراقبة على تكامل

.Canvas

كشفت Turnitin، مزوّد خدمات فحص الانتحال التي تعتمد عليها آلاف المؤسسات التعليمية والبحثية حول العالم، عن هجوم سيبراني طال بعض أنظمتها المواجهة للعملاء. والشركة تابعة لـ Advance Publications.

ما أعلنته الشركة

قال الرئيس التنفيذي Chris Caren في رسالة نُشرت على موقع الشركة بتاريخ 23 نوفمبر إن Turnitin رصدت نشاطاً غير مصرح به. وقد فعّلت الشركة خطة الاستجابة للحوادث، وأبلغت الجهات المعنية، وبدأت تحقيقاً بدعم من خبراء سيبرانيين خارجيين. وتؤكد أن أنظمتها تعمل بالكامل وأن استخدامها آمن، وأن الأنظمة المتأثرة لا تجمع وثائق الهوية الحكومية ولا المعلومات المالية للمؤسسات. وتتواصل المراقبة بينما يستمر التحقيق في طبيعة الحادث ونطاقه.

وتشمل الأنظمة المواجهة للعملاء بوابة تسليم الطلاب، وواجهة التصحيح للمدرّسين، وواجهات برمجة التكامل للمؤسسات، ولوحات التقارير. ولم تذكر الشركة هل اختُرق أي منها، ولا أيها.

ما لا يزال غير معروف

لم تبيّن الشركة هل جرى الوصول إلى بيانات، ولا عدد العملاء الذين قد يكونون متأثرين. وذكرت جامعة كولورادو بولدر أنها على تواصل مع Turnitin لمعرفة ما إذا كانت معلوماتها قد تعرضت للخطر، وأنه لا يوجد حالياً ما يدل على انكشاف بيانات الطلاب أو المدرّسين أو واجباتهم. ولأن الوصول إلى Turnitin يتم غالباً عبر تكامل مع Canvas، أضافت الجامعة مراقبة للتأكد من سلامة Canvas.

لماذا يهم المؤسسات

ينبغي للجهات التعليمية والبحثية التي تعتمد على Turnitin، مباشرة أو عبر منصة تعلّم، أن تتعامل مع الأمر بوصفه حادثاً لدى طرف ثالث لا يزال يتطور. فالمعلومات المتاحة محدودة، ولم يُؤكد أي أثر على مؤسسة بعينها. والنهج المتزن هو طلب الإيضاح من المورّد ومراقبة نقاط التكامل.

ما يجب فعله الآن

1. تأكد مما إذا كانت مؤسستكم تستخدم Turnitin مباشرة أو عبر تكامل مع نظام إدارة التعلم، وحدد مالك الخدمة في الأعمال.
2. اطلبوا من Turnitin كتابياً إفادتكم بما إذا تأثرت بيئتكم أو بياناتكم، مع تزويدكم بالمستجدات.
3. فعّلوا مراقبة إضافية على التكاملات وواجهات البرمجة بين نظام التعلم وTurniting، وراجعوا السجلات بحثاً عن نشاط غير معتاد.
4. راجعوا أنواع البيانات المشاركة مع الخدمة وتأكدوا من توافقها مع تصنيف البيانات والتزامات نظام حماية البيانات الشخصية (PDPL).
5. راجعوا بنود الحوادث والإشعار في عقود الأطراف الثالثة، وأعدّوا إحاطة داخلية موجزة للقيادة.