المفوضية الأوروبية تؤكد تسرب بيانات شخصية في هجوم بمساعدة الذكاء الاصطناعي استهدف منصة EU Academy



أكدت المفوضية الأوروبية أن هجوماً سيبرانياً بمساعدة الذكاء الاصطناعي كشف أسماء مستخدمي منصة EU Academy وعناوين بريدهم الإلكتروني، والتحقيق لا يزال جارياً.

- رُصد الهجوم في 22 أكتوبر، وأدى في البداية إلى إيقاف مؤقت لعدة تطبيقات.
- كشف التحقيق لاحقاً عن اختراق في EU Academy، وهي منصة تعليمية يستخدمها أشخاص من خارج المفوضية.
- شمل التسرب أسماء المستخدمين وعناوين بريدهم الإلكتروني، ولا يزال نطاقه الكامل قيد التحقيق.
- عُلّق الوصول إلى المنصة وجرى إبلاغ المشرف الأوروبي على حماية البيانات.
- لم تُحسم نسبة الهجوم بعد؛ وأفادت Euronews بوجود اشتباه في مجموعة مدعومة من الصين،

> ولم تحدد المفوضية الأداة المستخدمة.

أكدت المفوضية الأوروبية أن الهجوم السيبراني الذي أعلنت عنه الأسبوع الماضي أدى إلى تعرّض معلومات شخصية للاختراق. وكانت قد ذكرت في البداية أنها لم تجد دليلًا على تأثر بيانات موظفيها، وأوقفت عدداً من التطبيقات مؤقتاً.

ما هو معروف

ذكر متحدث باسم المفوضية أن التحقيق كشف عن اختراق طال منصة EU Academy، وهي منصة تعليمية عبر الإنترنت يستخدمها أشخاص من خارج المفوضية للالتحاق بدورات عن سياسات الاتحاد الأوروبي. وتشمل البيانات المكشوفة أسماء المستخدمين وعناوين بريدهم الإلكتروني، فيما لا يزال النطاق الكامل قيد الفحص. وقد عُلّق الوصول إلى المنصة، وجرى إبلاغ المشرف الأوروبي على حماية البيانات.

ولم تتواصل المفوضية مع المتأثرين فردياً لأن حجم التسرب لم يتحدد بعد، واكتفت بإشعار عام لجميع مستخدمي الموقع. وكان الهجوم قد رُصد في 22 أكتوبر، وقالت المفوضية الأسبوع الماضي إنه احتُوي إلى حد كبير، لكنها امتنعت يوم الاثنين عن تأكيد انتهاء الحادثة.

النسبة ودور الذكاء الاصطناعي

ذكرت المفوضية أن الذكاء الاصطناعي استُخدم في الهجوم دون أن تسمّي الأداة. وأفادت Euronews بأن المفوضية تشتبه في مجموعة مدعومة من الصين، وبأن الهجوم لم يُحتوَ بالكامل بعد، وأن الاشتباه يستند جزئياً إلى استخدام Artex، وهو إطار اختبار اختراق مدعوم بالذكاء الاصطناعي ذو جذور صينية. وتقول المفوضية إن النسبة لن تُحسم إلا بعد انتهاء التحقيق، لذا ينبغي التعامل مع هذه المعلومات على أنها غير مؤكدة.

لماذا يهم ذلك

تبيّن الحادثة أن النتيجة الأولية بعدم تأثر البيانات الشخصية قد تتغير مع تقدم التحقيق. كما تُظهر أن المنصات الموجهة لمستخدمين خارجيين، مثل بوابات التدريب أو العملاء، قد تحتفظ ببيانات شخصية تستحق الحماية نفسها التي تحظى بها الأنظمة الأساسية.

ما يجب فعله الآن

1. حصر المنصات المواجهة للإنترنت (التدريب، العملاء، الشركاء) وتوثيق البيانات الشخصية التي تحتفظ بها كل منصة.
2. مراجعة خطط الاستجابة للحوادث بحيث تُعدّ عبارة «لا أثر على البيانات الشخصية» الأولية مؤقتة إلى حين اكتمال تحديد النطاق.
3. التأكد من جاهزية خطوات تقييم الاختراق والإبلاغ وفق نظام حماية البيانات الشخصية (PDPL)، بما في ذلك التواصل مع سدايا، في الحوادث التي تشمل الأسماء والبريد الإلكتروني.
4. إعداد نموذج إشعار عام للمستخدمين للحالات التي يتعذر فيها تحديد المتأثرين بعد.
5. إدراج سيناريوهات الهجمات المدعومة بالذكاء الاصطناعي في نمذجة التهديدات واختبارات الكشف للتطبيقات المواجهة للإنترنت.