المفوضية الأوروبية تؤكد تعرضها لهجومٍ سيبراني بمساعدة الذكاء الاصطناعي عطّل عدداً من خدماتها



أكدت المفوضية الأوروبية أن هجوماً بمساعدة الذكاء الاصطناعي رُصد في 22 أكتوبر عطّل عدة خدمات. الهجوم محتوى إلى حد كبير، ولا دليل حتى الآن على اختراق بيانات الموظفين، والتحقيق مستمر.

- رُصد الهجوم في 22 أكتوبر وتأكد في 26 أكتوبر، وتقول المفوضية إنه محتوى إلى حد كبير.
- أوقفت المفوضية عدة تطبيقات مؤقتاً كإجراء وقائي، وأُعيد تشغيل معظمها.
- وفق Politico استمر التعطل أكثر من 10 أيام وشمل Sysper وMyPMO وأنظمة الترجمة.
- أكدت المفوضية استخدام أداة ذكاء اصطناعي دون تسميتها أو نسبة الهجوم إلى جهة معروفة، ولا علم لها بطلب فدية.
- كان CERT-EU قد حذّر سابقاً من استخدام جهات التهديد إطار الاختبار الاختراقي Artex المعتمد على الذكاء الاصطناعي، متوقعاً هجمات آلية أسرع وأوسع نطاقاً.

أكدت المفوضية الأوروبية تعرضها لهجوم سيبراني استخدم فيه المهاجمون أداة ذكاء اصطناعي. وبحسب المتحدث باسمها توماس ريغنييه، رُصد الهجوم في 22 أكتوبر وتأكد في 26 أكتوبر، وهو محتوى إلى حد كبير بينما لا يزال التحقيق جارياً.

ما الذي حدث

كإجراء وقائي، أوقفت المفوضية عدة تطبيقات مؤقتاً، وأُعيد تشغيل معظمها. وقال ريغنييه إن التحقيق لم يجد دليلًا على اختراق بيانات يطال موظفي المفوضية. في المقابل، تفيد Politico بأن المهاجمين ربما اطلعوا على كميات كبيرة من البيانات، وبأن التعطل استمر أكثر من 10 أيام وأثّر في منصة الموارد البشرية Sysper ونظام التعويضات الطبية MyPMO وأنظمة الترجمة.

ولم تسمِّ المفوضية الأداة المستخدمة، ولم تنسب الهجوم إلى جهة معروفة، وذكرت أنها لا تعلم بوجود طلب فدية.

السياق الأوسع

جاء الإعلان بعد نحو أسبوعين من تحذير CERT-EU من استخدام جهات تهديد للإطار Artex، وهو إطار اختبار اختراقي مدعوم بالذكاء الاصطناعي، ضد الجهات التي يخدمها. وقدّر الفريق أن إتاحة الإطار للعموم سترفع على الأرجح وتيرة اعتماده لدى المهاجمين، ما يعني هجمات آلية أكثر تكراراً وأسرع وأوسع نطاقاً ونسبة نجاح أعلى. ويضيف المصدر أن Artex استُخدم ضد جهات منها Barracuda وRailway وعملاء ConnectWise.

لماذا يهم ذلك

لا يربط المصدر حادثة المفوضية بـ Artex. لكنها تُظهر أن الاختراق المدعوم بالذكاء الاصطناعي بات واقعاً موثقاً ضد مؤسسة عامة كبرى، وأن الاحتواء قد يعني إيقاف تطبيقات حيوية لأيام. وعلى المؤسسات الخاضعة للتنظيم أن تعدّ ذلك دافعاً لمراجعة سرعة الكشف وخيارات العزل وأولويات التعافي، لا سبباً للقلق.

ما يجب فعله الآن

1. راجعوا حدود الكشف والتنبيه بحيث يُرصد النشاط الآلي السريع ويُصعَّد خلال ساعات لا أيام.
2. حدّدوا مسبقاً التطبيقات التي يمكن عزلها أو إيقافها أثناء الحادثة، مع توثيق المسؤولين ومسارات الاعتماد.
3. اختبروا استعادة منصات الموارد البشرية والمزايا وغيرها من المنصات الداخلية، وأكدوا أولويات الاستعادة في خطط استمرارية الأعمال.
4. قيّموا التعرض لأدوات الاختبار الاختراقي المدعومة بالذكاء الاصطناعي عبر فحوص دورية لسطح الهجوم الخارجي ومعالجة الأنظمة المكشوفة للإنترنت دون تأخير.
5. حدّثوا أدلة الاستجابة للحوادث لتشمل الهجمات بمساعدة الذكاء الاصطناعي، وكيفية تقدير تعرض البيانات عندما تكون الأدلة غير مكتملة.