اختراق مُبلَّغ عنه لنظام غير سري في وكالة الاستخبارات المركزية الأمريكية يتعلق بالاستخبارات مفتوحة المصدر



أفاد مصدر مطلع لوكالة أسوشيتد برس باختراق نظام غير سري في وكالة الاستخبارات المركزية يعالج الاستخبارات مفتوحة المصدر. لم تُمسّ معلومات سرية وجرت المعالجة، ولم يُعرف المهاجم ولا البيانات المتأثرة.

- قال مصدر مجهول لوكالة أسوشيتد برس إن الاختراق طال نظاماً غير سري في الوكالة يُستخدم للاستخبارات مفتوحة المصدر، وكانت نيويورك تايمز أول من نشر الخبر.
- أكد المصدر أن الحادثة لم تتضمن معلومات سرية وأنها عولجت.
- لا يتضح ما المعلومات التي تعرضت للاختراق ولا الجهة المسؤولة.
- قد تمنح المعلومات مفتوحة المصدر المحللين رؤية مهمة بمفردها أو عند دمجها مع استخبارات سرية.
- يأتي الخبر بعد أعطال أخرى في أنظمة أمريكية، ونفت الإدارة أنها هجوم منسق وربطتها بتسارع

التحديث والترقيع.

أفاد شخص مطلع على الحادثة، تحدث إلى وكالة أسوشيتد برس شريطة عدم كشف هويته، بأن نظاماً غير سري في وكالة الاستخبارات المركزية الأمريكية تعرض لاختراق. وكانت صحيفة نيويورك تايمز أول من نشر الخبر. وقال المصدر إن الحادثة لم تتضمن معلومات سرية وإن المشكلة عولجت.

ما المعروف حتى الآن

يتعامل النظام المتأثر مع الاستخبارات مفتوحة المصدر، أي جمع وتحليل بيانات متاحة للعامة من الإنترنت والأقمار الصناعية التجارية ووسطاء البيانات الخاصين. وهذه المعلومات عادةً عامة أو شبه عامة، لكنها قد تمنح المحللين رؤية مهمة بمفردها أو حين تُدمج مع استخبارات من برامج سرية. ولم يحدد المصدر المعلومات التي تعرضت للاختراق، ولم تُعرف الجهة المسؤولة. ويستند الخبر إلى مصدر واحد مجهول.

السياق الأوسع

يأتي الخبر بعد حوادث معطّلة عدة في الولايات المتحدة، منها توقف شبكة سرية تابعة لوكالة الأمن القومي، واختراق ظاهر لقاعدة بيانات إنفاذ القانون لدى مكتب التحقيقات الفيدرالي قيد التحقيق، وتوقف الرحلات الجوية، وأعطال في أنظمة أبل وجيه بي مورغان تشيس ومايكروسوفت. وتقول الإدارة الأمريكية إن هذه الحوادث ليست هجوماً سيبرانياً منسقاً، وعزا مدير الاستخبارات الوطنية جاي كلايتون الأعطال في معظمها إلى التسرع في ترقيع الأنظمة وتحديثها لمواجهة مهاجمين يستخدمون أدوات ذكاء اصطناعي متقدمة.

الأهمية للجهات المنظَّمة

الدرس لا يخص جهة بعينها. فالأنظمة المصنفة منخفضة الحساسية والبيانات العامة أو التجارية المجمَّعة قد تبقى ذات قيمة للخصم، كما أن التغيير السريع قد يخلق مخاطره الخاصة. ويمكن للمؤسسات في المملكة اعتبار الخبر دافعاً لمراجعة مدى صحة هذه الافتراضات في بيئاتها.

ما يجب فعله الآن

1. مراجعة كيفية عزل الأنظمة المصنفة منخفضة الحساسية أو غير السرية عن البيئات الأساسية والحساسة.
2. حصر الأنظمة التي تجمع بيانات عامة أو تجارية أو من أطراف ثالثة وتقييم ما قد يستنتجه الخصم منها.
3. التأكد من أن برامج الترقيع والتحديث تشمل الاختبار وإدارة التغيير وخطط التراجع.
4. التحقق من أن خطط الاستجابة للحوادث تغطي الأنظمة خارج النطاق الحساس الرئيس، بما في ذلك التصعيد والإبلاغ للجهات التنظيمية.
5. إحاطة الإدارة العليا بأن الخبر يستند إلى مصدر مجهول واحد وأن النطاق والجهة المسؤولة لم يتأكدا.