تقارير: مكتب التحقيقات الفيدرالي يحقق في اختراق ثانٍ يطال قاعدة بيانات NCIC



تفيد تقارير بأن مكتب التحقيقات الفيدرالي يحقق في هجوم سيبراني استهدف المركز الوطني للمعلومات الجنائية، وهو قاعدة بيانات مشتركة للجهات الأمنية الأمريكية. ولم يتأكد الحادث رسميًا.

- نقلت CNN وAssociated Press عن مصادر أن الهجوم على NCIC وقع يوم الخميس، ولم يعلّق المكتب.
- تستخدم الجهات المحلية وعلى مستوى الولايات والجهات الاتحادية قاعدة NCIC لتبادل معلومات عن المجرمين والمطلوبين وأوامر القبض والمفقودين.
- إذا تأكد الحادث فسيكون الثاني للمكتب هذا العام بعد اختراق مجموعة ShinyHunters لموقع التوظيف في سبتمبر.
- أبلغت جهات أمريكية أخرى عن حوادث هذا العام، منها ATF ووزارات الدفاع والنقل والزراعة.

تفيد تقارير، نقلاً عن مصادر لدى CNN وAssociated Press، بأن مكتب التحقيقات الفيدرالي يحقق في اختراق يتعلق بالمركز الوطني للمعلومات الجنائية (NCIC). ويُقال إن الهجوم وقع يوم الخميس. ولم يرد المكتب على طلبات التعليق، ولذلك يبقى الحادث غير مؤكد.

ما المعروف حتى الآن

NCIC قاعدة بيانات تستخدمها الجهات المحلية وجهات الولايات والجهات الاتحادية في الولايات المتحدة لتبادل المعلومات عن المجرمين والتحقيقات. وتضم بيانات عن أوامر القبض القائمة ومعلومات حساسة ذات قيمة للمجرمين. ولا يوضح المصدر كيف وقع الهجوم أو ما البيانات التي جرى الوصول إليها أو الجهة المسؤولة.

وذكر الرئيس دونالد ترامب أنه اطّلع على الحادث ووصفه بأنه غير جيد، وأضاف أن الاختراق قد يتيح للعامة الوصول إلى ملفات تحقيق تخصه.

السياق الأوسع

إذا تأكد الحادث فسيكون الثاني للمكتب هذا العام. ففي سبتمبر اخترقت مجموعة ShinyHunters موقع التوظيف التابع للمكتب، وزُعم أنها سرقت معلومات عن جميع موظفيه، وجرى توقيف عدة أشخاص في التحقيق.

وتأثرت جهات حكومية أمريكية أخرى هذا العام؛ إذ تعطلت منصة تستخدمها محاكم الإفلاس الاتحادية، ووصفت ATF هجوم فدية في أغسطس بأنه حادث كبير. كما أبلغت وزارتا الدفاع والنقل عن حوادث، وأوقفت وزارة الزراعة أنظمة المدفوعات بعد هجوم الأسبوع الماضي.

الصلة بالمؤسسات السعودية

لا يشير التقرير إلى تعرض جهات سعودية. ومع ذلك فهو تذكير بأن قواعد البيانات المشتركة بين جهات عدة تركّز المخاطر، وأن تكرار الحوادث قد يطال حتى الجهات ذات الموارد الكبيرة.

ما يجب فعله الآن

1. راجع قواعد البيانات المشتركة أو متعددة الأطراف التي تعتمد عليها مؤسستكم ومن يملك صلاحية الوصول إليها.
2. تأكد من تقييد الوصول إلى الأنظمة المشتركة الحساسة بحسب الدور، مع مصادقة قوية وتسجيل للأحداث.
3. تحقق من أن خطة الاستجابة للحوادث تغطي اختراق الأطراف الثالثة والمنصات المشتركة، بما في ذلك التزامات الإبلاغ.
4. تابع المصادر الرسمية للحصول على تفاصيل مؤكدة قبل استخلاص نتائج أو إحاطة الإدارة العليا.