مكتب التحقيقات الفيدرالي يحقق في اختراق محتمل لقاعدة بيانات العدالة الجنائية الوطنية



يحقق مكتب التحقيقات الفيدرالي في اختراق محتمل لقاعدة بيانات NCIC للعدالة الجنائية، بحسب مصدر مطلع. ولم يتضح نطاق الحادث، ورفض المكتب التعليق.

- أفاد شخص مطلع لوكالة أسوشيتد برس بأن المكتب يحقق في اختراق محتمل لمركز معلومات الجريمة الوطني (NCIC).
- تضم القاعدة سجلات عن الفارين والمفقودين والسجل الجنائي والممتلكات المسروقة، وتتاح لجهات إنفاذ القانون المحلية والولائية والفيدرالية.
- لم يتضح نطاق المشكلة فور الإعلان، ورفض المكتب التعليق.
- لا مؤشر فوريًا على ارتباط الحادث بأعطال رقمية حديثة في القطاعين الحكومي والخاص، وقد عزاها مسؤولون إلى ترقيات وإصلاحات دورية.
- كان المكتب هدفًا متكررًا للمخترقين، ومنه ادعاء مجموعة ShinyHunters في سبتمبر وتحقيق

في نظام داخلي في مارس.

ما الذي نعرفه

يحقق مكتب التحقيقات الفيدرالي في اختراق محتمل لمركز معلومات الجريمة الوطني المعروف باسم NCIC، بحسب شخص مطلع تحدث إلى وكالة أسوشيتد برس شريطة عدم كشف هويته. وكانت CNN أول من نشر الخبر. ورفض المكتب التعليق، ولم يتضح نطاق المشكلة فور الإعلان.

وNCIC قاعدة بيانات محوسبة للمعلومات الجنائية تتاح لجهات إنفاذ القانون المحلية والولائية والفيدرالية، وتتضمن سجلات عن الفارين والمفقودين والسجل الجنائي والممتلكات المسروقة.

السياق

يأتي الخبر بعد سلسلة أعطال رقمية في القطاعين الحكومي والخاص. وقال مسؤولون في إدارة ترمب إنها نتجت عن ترقيات روتينية وإصلاح ثغرات وليس عن هجوم سيبراني. ولا يوجد مؤشر فوري على صلة الحادث الحالي بها.

وسبق أن استُهدف المكتب. ففي سبتمبر أعلنت مجموعة ShinyHunters حصولها على كمية كبيرة من بيانات موظفي المكتب والمتقدمين للوظائف، واختراق بوابة التوظيف. وفي مارس أعلن المكتب تحقيقه في نشاط مشبوه على نظام داخلي يحتوي معلومات حساسة عن عمليات المراقبة والتحقيقات.

أهمية الخبر للمؤسسات في المملكة

لم يذكر المصدر أي أثر على السعودية. ومع ذلك يذكّر الحادث المؤسسات التي تحتفظ بسجلات حساسة مشتركة يصل إليها أطراف عديدة بأن حجم التعرض يعتمد على اتساع الصلاحيات وجودة المراقبة. والتفاصيل غير مؤكدة، لذا ينبغي التعامل مع ما نُشر بوصفه أوليًا وتجنب الاستنتاج بشأن السبب أو الأثر قبل صدور معلومات رسمية.

ما يجب فعله الآن

1. راجع الجهات الداخلية والخارجية التي يحق لها الوصول إلى قواعد البيانات الحساسة المشتركة، وألغِ الصلاحيات غير الضرورية.
2. تأكد من أن السجلات والتنبيهات تغطي الاستعلامات وعمليات التصدير الكبيرة في أنظمة السجلات الأكثر حساسية.
3. تحقق من أن خطة الاستجابة للحوادث تشمل حالات غير واضحة النطاق، بما فيها التصعيد والإبلاغ للجهات التنظيمية.
4. تابع التحديثات الرسمية بدل التقارير غير المؤكدة قبل تغيير أي ضوابط أو إحاطة مجلس الإدارة.