وكالة فرانس برس تُوقف منصة AFP Forum بعد هجوم سيبراني



أكدت وكالة فرانس برس تعرّض منصة AFP Forum، التي يستخدمها عملاؤها لتنزيل موادها، لهجوم سيبراني. أُوقفت المنصة احترازياً وبقيت متوقفة يوم الجمعة، ولم يُعرف المهاجم ولا حجم الأثر.

- استُهدفت منصة AFP Forum، التي تستخدمها المؤسسات الإعلامية لتصفح وتنزيل نصوص الوكالة وصورها ومقاطعها، خلال الليل.
- رصدت الوكالة الاختراق وبادرت إلى احتوائه وأوقفت المنصة احترازياً.
- يساعد خبراء أمن سيبراني خارجيون في التحقيق.
- لم تُحدَّد الجهة المهاجمة ولا موعد لاستعادة الخدمة، ولا يزال غير واضح هل جرى الوصول إلى بيانات أو تأثرت أنظمة أخرى.
- سبق أن أعلنت الوكالة هجوماً في سبتمبر 2024 عطّل بعض خدمات إيصال المحتوى.

تعرضت وكالة فرانس برس (AFP) لهجوم سيبراني خلال الليل، بحسب رسالة داخلية إلى الموظفين نقلتها الوكالة في تغطيتها الخاصة. وكان الهدف منصة AFP Forum، وهي منصة إلكترونية تستخدمها المؤسسات الإخبارية لتصفح نصوص الوكالة وصورها ومقاطع الفيديو وتنزيلها.

ما المعروف

تفيد الوكالة بأن فرقها احتوت الاختراق فور رصده وأوقفت AFP Forum احترازياً. وبقيت المنصة غير متاحة يوم الجمعة وتعرض إشعار صيانة بعدة لغات. وبحسب تقارير إعلامية فرنسية، تتيح الوكالة للمشتركين وسائل بديلة للوصول إلى المحتوى في هذه الأثناء. وتجري الوكالة التحقيق بمساعدة خبراء أمن سيبراني خارجيين.

ما غير المعروف

لم تكشف الوكالة عن الجهة المنفذة ولا عن موعد عودة الخدمة. ولا يزال غير واضح هل جرى الوصول إلى معلومات حساسة أو تأثرت أنظمة أخرى. ولم ترد الوكالة على طلب التعليق. وليست هذه الحادثة الأولى؛ ففي سبتمبر 2024 رصدت الوكالة هجوماً على أنظمتها المعلوماتية عطّل بعض الخدمات المستخدمة لإيصال المحتوى إلى المشتركين، ولم يُنسب علناً إلى جهة محددة.

أهمية الحادثة

تُظهر الحادثة كيف يمكن لمنصة خارجية يعتمد عليها العملاء أن تصبح نقطة تعطّل واحدة، وأن الإيقاف الاحترازي خيار احتواء مشروع له أثر على الخدمة. وتصلح الحادثة دافعاً للمؤسسات التي تقدم بياناتها أو محتواها لعملائها عبر بوابات إلكترونية لاختبار ترتيبات الاحتواء والبدائل لديها.

ما يجب فعله الآن

1. حصر البوابات ومنصات التنزيل الموجهة للعملاء والتأكد من أن لكل منها مالكاً معيناً وجهة اتصال عند الحوادث.
2. اعتماد مسبق لمعايير وصلاحية إيقاف أي منصة خارجية كإجراء احتواء.
3. إعداد قنوات بديلة واختبارها ليتمكن العملاء من استلام المحتوى أو البيانات الأساسية أثناء التوقف.
4. التحقق من كفاية سجلات الأحداث على المنصات المواجهة للإنترنت لتحديد الوصول إلى البيانات لاحقاً.
5. مراجعة التزامات الإبلاغ للجهة التنظيمية والعملاء المتأثرين عند تأكد الاختراق، وتدريب الفرق عليها بتمرين نظري.