الفيفا تؤكد تعرضها لهجوم سيبراني طال بيانات شخصية وبيانات أعمال



أعلن الفيفا أن مهاجمين وصلوا إلى مجموعة محدودة من البيانات الشخصية وبيانات الأعمال، وأنه يتعاون مع جهات إنفاذ القانون. ولم يوضح موعد الهجوم ولا طبيعة البيانات بدقة.

- يقول الفيفا إن مهاجمين وصلوا إلى مجموعة محدودة من البيانات الشخصية وبيانات الأعمال.
- يتعاون الفيفا مع الجهات المختصة، ومنها جهات إنفاذ القانون.
- لم يحدد الفيفا وقت وقوع الهجوم ولا الطبيعة الدقيقة للبيانات.
- نشرت مجموعة تسمي نفسها Handsome Boy Hacking Club لقطة شاشة لملفات تزعم أنها للفيفا على منصة X، ثم بدا أنها تبنّت الاختراق.
- تحدث منشور عن تسريب أكثر من 12 غيغابايت من الوثائق الداخلية، وهذا ادعاء لم يؤكده الفيفا.

أعلن الاتحاد الدولي لكرة القدم (الفيفا) أنه تعرض لهجوم سيبراني تمكن فيه مهاجمون من الوصول إلى ما وصفه بمجموعة محدودة من البيانات الشخصية وبيانات الأعمال. وجاء ذلك في بيان أرسله إلى وكالة أسوشييتد برس ونقلته SecurityWeek.

ما المعروف حتى الآن

يقول الفيفا إنه يعمل بشكل وثيق مع الجهات المختصة، ومنها جهات إنفاذ القانون. ولم يذكر متى وقع الهجوم، ولم يحدد الطبيعة الدقيقة للمعلومات المعنية. وأدان الحصول غير المشروع على البيانات ونشرها، ولا سيما البيانات الشخصية، واعتبر ذلك انتهاكاً جسيماً للخصوصية قد تترتب عليه عواقب كبيرة على الأفراد المتضررين.

وكانت مجموعة تسمي نفسها Handsome Boy Hacking Club قد نشرت الأسبوع الماضي على منصة X لقطة شاشة لما زعمت أنها ملفات للفيفا. وبعد ثلاثة أيام بدا أنها تتبنى الاختراق، إذ ردّت على منشور تحدث عن تسريب أكثر من 12 غيغابايت من الوثائق الداخلية. وحجم التسريب ومحتواه مصدرهما هذه الادعاءات ولم يؤكدهما الفيفا.

أهمية الخبر للجهات المنظمة

تذكّر الحادثة بأن المنظمات التي تتعامل مع شبكة واسعة من الشركاء والموردين وأصحاب المصلحة تحتفظ ببيانات شخصية وتجارية قد تُنشر بسرعة بعد سرقتها. ولا تزال تفاصيل كثيرة غير معلنة، لذا ينبغي للمؤسسات التي ترتبط بعلاقات مع هيئات دولية كبرى ألا تفترض وجود أثر أو انعدامه، وأن تراجع انكشافها بهدوء.

ما يجب فعله الآن

1. تحقق مما إذا كانت مؤسستكم تشارك بيانات شخصية أو تجارية مع الفيفا أو الجهات التابعة له، واطلبوا من جهات الاتصال المعنية أي إشعار تعتزم إصداره.
2. راجعوا الأطراف الثالثة التي تحتفظ ببيانات موظفيكم أو عملائكم أو شركائكم، وتأكدوا من التزاماتها التعاقدية بالإبلاغ عن الحوادث.
3. إذا كان من المحتمل أن تتضمن البيانات المسربة بيانات تخصكم، فقيّموا الأمر وفق نظام حماية البيانات الشخصية (PDPL) ومتطلبات الإشعار لدى الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا)، ووثّقوا القرار.
4. نبّهوا الموظفين المحتمل استهدافهم برسائل تصيد تستند إلى وثائق مسربة، وذكّروهم بالإبلاغ عن الرسائل المشبوهة.
5. تأكدوا من أن خطة الاستجابة للحوادث تغطي نشر المهاجمين للبيانات المسروقة على وسائل التواصل، بما في ذلك الجوانب الإعلامية والقانونية.