فيفا تؤكد تعرضها لاختراق بينما تزعم مجموعة قرصنة تسريب سجلات داخلية



أكدت فيفا أن مخترقين وصلوا إلى مجموعة محدودة من المعلومات الشخصية وبيانات الأعمال.
وتزعم مجموعة HBHC أنها سحبت بيانات من بيئة Microsoft لدى فيفا، دون أن تحدد فيفا نوع البيانات أو توقيت الحادثة.

- أكدت فيفا يوم الخميس أن المهاجمين وصلوا إلى مجموعة محدودة من المعلومات الشخصية وبيانات الأعمال، وأنها تتعاون مع الجهات الأمنية.
- لم تذكر فيفا توقيت الهجوم ولا طبيعة المعلومات التي أُخذت.
- نشرت مجموعة تسمي نفسها HBHC (Handsome Boy Hacking Club) قبل أسبوع لقطة شاشة على منصة X وادّعت أن البيانات مصدرها بيئة Microsoft لدى فيفا.
- تذكر المجموعة أن المواد تشمل وثائق هوية وسجلات هجرة ومعلومات عن مسؤولين تنفيذيين وبيانات مالية ووثائق قانونية، وتقول إن دافعها مالي.

- أعلنت رابطة LaLiga في الأسبوع نفسه عن اختراق منفصل لإحدى منصات خدمات الجماهير.

ما هو معروف

أكدت فيفا يوم الخميس أن مجرمين إلكترونيين وصلوا إلى أنظمتها وحصلوا على ما وصفته بمجموعة محدودة من المعلومات الشخصية وبيانات الأعمال. وذكرت أنها تتعاون مع الجهات المختصة، ومنها الجهات الأمنية. ولم تُفصح عن وقت الاختراق ولا عن نوع البيانات المسحوبة.

جاء التأكيد بعد أسبوع من منشور على منصة X لمجموعة تسمي نفسها Handsome Boy Hacking Club (HBHC)، نشرت فيه لقطة شاشة قالت إنها لملفات تعود إلى فيفا.

ما تدّعيه المجموعة

تقول المجموعة إن البيانات صُدّرت من بيئة Microsoft لدى فيفا، وتتضمن نسخة كاملة من أنظمة الحوكمة الداخلية إضافة إلى مستندات ولقطات شاشة من خدمات متنوعة. ويذكر المنشور وثائق هوية وسجلات هجرة ومعلومات عن مسؤولين تنفيذيين وبيانات مالية ووثائق قانونية. وهذه ادعاءات المجموعة نفسها، ولم يتحقق المصدر منها بصورة مستقلة.

وتُوصف HBHC بأنها مجموعة حديثة نسبياً، إذ أدرجت أول ضحية على موقع التسريبات في 19 نوفمبر. وتقول إن دافعها مالي بحت وتَعِد بتسريبات أخرى. وفي سياق منفصل، أكدت LaLiga هذا الأسبوع اختراق إحدى منصات خدمات الجماهير وسرقة بيانات شخصية.

لماذا يهم المؤسسات في المملكة

تذكّر الحادثة بأن بيئات التعاون السحابية وأنظمة الحوكمة تضم سجلات هوية وسجلات قانونية ومالية تجذب المجموعات الباحثة عن الربح. وعلى المؤسسات التي تتعامل مع هيئات دولية أو منظمات رياضية أو شركاء فعاليات أن تراجع ما شاركته من بيانات معهم، وأن تكون مستعدة للتصرف إذا تعرض أحد الشركاء لحادثة.

ما يجب فعله الآن

1. احصر البيانات الشخصية والمالية التي شاركتها مع هيئات دولية ومنظمي فعاليات وشركاء رياضيين، وتأكد من كيفية حمايتها لدى كل شريك.
2. راجع ضوابط الوصول والتسجيل وتصدير البيانات في بيئة Microsoft السحابية لديك، وفعّل التنبيه عند التصدير الكبير من أنظمة الحوكمة والمستندات.
3. تحقق من أن عقود الأطراف الثالثة تُلزم بالإبلاغ السريع عن الحوادث وتحدد جهات الاتصال للتنسيق.
4. استعد لمتطلبات تقييم الحوادث والإبلاغ بموجب نظام حماية البيانات الشخصية (PDPL)، بما يشمل تحديد ما إذا كانت بيانات مقيمين في المملكة لدى شريك قد تتأثر.
5. نبّه التنفيذيين والموظفين المتعاملين مع وثائق الهوية والهجرة إلى مخاطر التصيد وانتحال الهوية التي تعقب التسريبات.