Bullhorn توقف منصتها للتوظيف عن العمل لاحتواء هجوم سيبراني



عطّلت شركة Bullhorn، مزوّدة برمجيات التوظيف، الوصول إلى منصتها لاحتواء هجوم سيبراني تسبب في انقطاع شامل. على العملاء الاستعداد لاستمرارية الأعمال ومتابعة تحديثات المزوّد.

- عطّلت Bullhorn، وهي شركة برمجيات للتوظيف، الوصول إلى منصتها.
- جاء الإجراء لاحتواء هجوم سيبراني.
- تسبب الهجوم في انقطاع شامل للأنظمة.
- لا يوضح المقتطف المتاح تفاصيل عن تسرب البيانات أو سبب الحادثة أو موعد الاستعادة.

ما الذي حدث

عطّلت Bullhorn، الشركة المزوّدة لبرمجيات التوظيف، الوصول إلى منصتها بهدف احتواء هجوم سيبراني. وقد أدى

الحادث إلى انقطاع طال أنظمتها بصورة شاملة.

ما الذي لا يزال غير معروف

لا يبيّن النص المتاح من المصدر كيف وصل المهاجمون إلى الأنظمة، ولا ما إذا تأثرت بيانات العملاء أو المرشحين، ولا موعد عودة الخدمات. وإلى أن يصدر المزوّد معلومات إضافية، ينبغي تجنب الافتراضات في أي اتجاه والتعامل مع الواقعة بوصفها قيد التطور.

أهمية الأمر للمؤسسات في المملكة

غالباً ما تحتفظ منصات التوظيف بيانات شخصية عن المرشحين والموظفين، وتدعم مسارات استقطاب تعتمد عليها الجهات. فإذا كانت مؤسسة سعودية أو أحد شركائها في التوظيف يستخدم هذه المنصة، فإن الانقطاع يمثل مسألة استمرارية أعمال، ويثير كذلك مخاطر الأطراف الثالثة وحماية البيانات الشخصية. والاستجابة الهادئة المنظمة أجدى من التكهن.

تتمثل الخطوات العملية في التأكد من كونكم عملاء للمنصة، وتحديد كيفية استمرار أعمال التوظيف يدوياً، ومتابعة بيانات المزوّد الرسمية، والاستعداد لتقييم أي أثر على البيانات الشخصية إذا أكد المزوّد حدوث تعرض لها.

ما يجب فعله الآن

1. تأكدوا مما إذا كانت مؤسستكم أو وكالات التوظيف المتعاقدة معها تستخدم Bullhorn.
2. فعّلوا مسارات توظيف يدوية أو بديلة لضمان استمرارية العمل.
3. تابعوا البيانات الرسمية من Bullhorn واطلبوا تحديثاً كتابياً عن الحادثة.
4. حدّدوا البيانات الشخصية للمرشحين والموظفين التي يحتفظ بها المزوّد لصالحكم.
5. استعدوا لتقييم التزامات الإشعار وفق نظام حماية البيانات الشخصية (PDPL) إذا أكد المزوّد تعرض البيانات.
6. سجّلوا الحادثة في سجل مخاطر الأطراف الثالثة.