SBC Medical Group تكشف عن اختراق يطال أكثر من مليوني شخص في اليابان



أبلغت SBC Medical Group هيئة الأوراق المالية الأمريكية بأن مهاجمين دخلوا منصة إلكترونية تديرها وسرقوا بيانات شخصية وطبية مرتبطة بعيادات في اليابان. وفي حادثة منفصلة طالت خدمة الحجز Tribeau، انكشفت بيانات نحو 19 ألف شخص.

- سُرقت البيانات الأساسية لـ 1,624,000 شخص، منها الأسماء ووسائل التواصل وتواريخ الميلاد وأرقام بطاقات المرضى ومعرّفات الأعضاء وإجابات الاستبيانات.
- فقدت فئات أصغر طلبات الحجز ومحتوى نماذج الاستفسار ووصف العلاجات وأسماء ملفات الصور ونصوص التقييمات؛ وطالت بيانات البطاقات الائتمانية 14 شخصًا، وقالت الشركة إن جميعها لم تعد تقبل دفعات إضافية.
- سُرقت كلمات مرور العملاء و20,000 سجل للموظفين تشمل الأسماء والمعرّفات وكلمات المرور، وتأثرت بيانات مصرفية وتقاعدية وضريبية لـ 459 موظفًا.

- اختراق منفصل لخدمة الحجز الخارجية Tribeau كشف حسابات المسؤولين وبيانات نحو 19 ألف شخص.
- تقول الشركة إنها عالجت الحادثتين: عزلت الخادم المتأثر وأخرجت المهاجمين وغيّرت كلمات مرور Tribeau.

كشفت SBC Medical Group Holdings، وهي شركة مقرها كاليفورنيا تقدم الاستشارات والإدارة والدعم التشغيلي للشركات الطبية والعيادات، في إفصاح لدى هيئة الأوراق المالية والبورصات الأمريكية عن اختراق يمس أكثر من مليوني شخص في اليابان.

ما الذي حدث

دخل مهاجمون إلى منصة إلكترونية تديرها الشركة، وطالوا قواعد بيانات تضم معلومات عملاء مرتبطة بعيادات محددة. ولا يزال التحقيق جاريًا، لكن الشركة أكدت أن بيانات شخصية وطبية تعرضت للاختراق على الأرجح.

وتشمل أكبر مجموعة 1,624,000 شخص سُرقت أسماؤهم وعناوينهم وأرقام هواتفهم وبريدهم الإلكتروني وتواريخ ميلادهم وجنسهم وأرقام بطاقات المرضى ومعرّفات العضوية وإجابات الاستبيانات. وفقدت مجموعات أخرى طلبات الحجز (255,416) ومحتوى نماذج الاستفسار (217,769) ووصف العلاجات وأسماء ملفات الصور (4,513) ونصوص التقييمات مع أسماء العلاجات (15,007). كما طالت بيانات البطاقات الائتمانية 14 شخصًا، وتقول الشركة إن تلك البطاقات لم تعد قادرة على تنفيذ دفعات.

كذلك سُرقت كلمات مرور العملاء و20,000 سجل للموظفين تتضمن الأسماء والمعرّفات وكلمات المرور. وتأثرت لدى 459 موظفًا مستندات التوظيف، ومنها بيانات الحسابات المصرفية والتقاعد والنماذج الضريبية.

حادثة الطرف الثالث

وفي حادثة منفصلة، وصل مهاجمون إلى حسابات المسؤولين في خدمة الحجز Tribeau واطلعوا على بيانات نحو 19 ألف شخص. ويفيد المشغّل بأن البريد الإلكتروني وعناوين السكن وبيانات البطاقات وكلمات المرور والسجلات الطبية الإلكترونية لم تكن ضمن هذه الحادثة.

وتقول الشركة إنها عالجت الحادثتين؛ فعزلت الخادم المتأثر وأخرجت المهاجمين وغيّرت كلمات مرور جميع العيادات التي تديرها على Tribeau. وما زالت تقيّم الأثر على أعمالها ووضعها المالي.

أهمية الأمر للجهات في المملكة

تبيّن الحالة أن منصة الإدارة ومزوّد الحجز وسجلات الموظفين قد تصبح جميعها نقاط انكشاف في آن واحد. وتحتفظ الجهات الصحية وشركاؤها في المملكة ببيانات مماثلة، ما يستدعي مراجعة ضوابطها.

ما يجب فعله الآن

1. حصر المنصات الإلكترونية وخدمات الحجز أو التواصل مع المرضى لدى أطراف ثالثة التي تحتفظ ببيانات المرضى أو العملاء، وتأكيد مالك كل منها.
2. مراجعة حسابات المسؤولين على منصات الموردين: فرض المصادقة متعددة العوامل، وحذف

الحسابات غير المستخدمة، وتغيير بيانات الاعتماد بعد أي حادثة لدى المورد.

3. التحقق من تخزين كلمات المرور بتجزئة قوية ومن عدم إعادة استخدام بيانات اعتماد الموظفين والعملاء عبر الأنظمة.
4. الحد من مدة الاحتفاظ بمستندات الموارد البشرية الحساسة، كالبيانات المصرفية والضريبية، وتقييد الوصول إليها.
5. التأكد من أن خطة الاستجابة للحوادث تغطي تقييم الاختراقات والإبلاغ عنها وفق نظام حماية البيانات الشخصية (PDPL)، بما فيها الحوادث الناشئة لدى الموردين.
6. إلزام الموردين بإخطارك فورًا بالحوادث ومشاركة نتائج تحليل السبب الجذري.