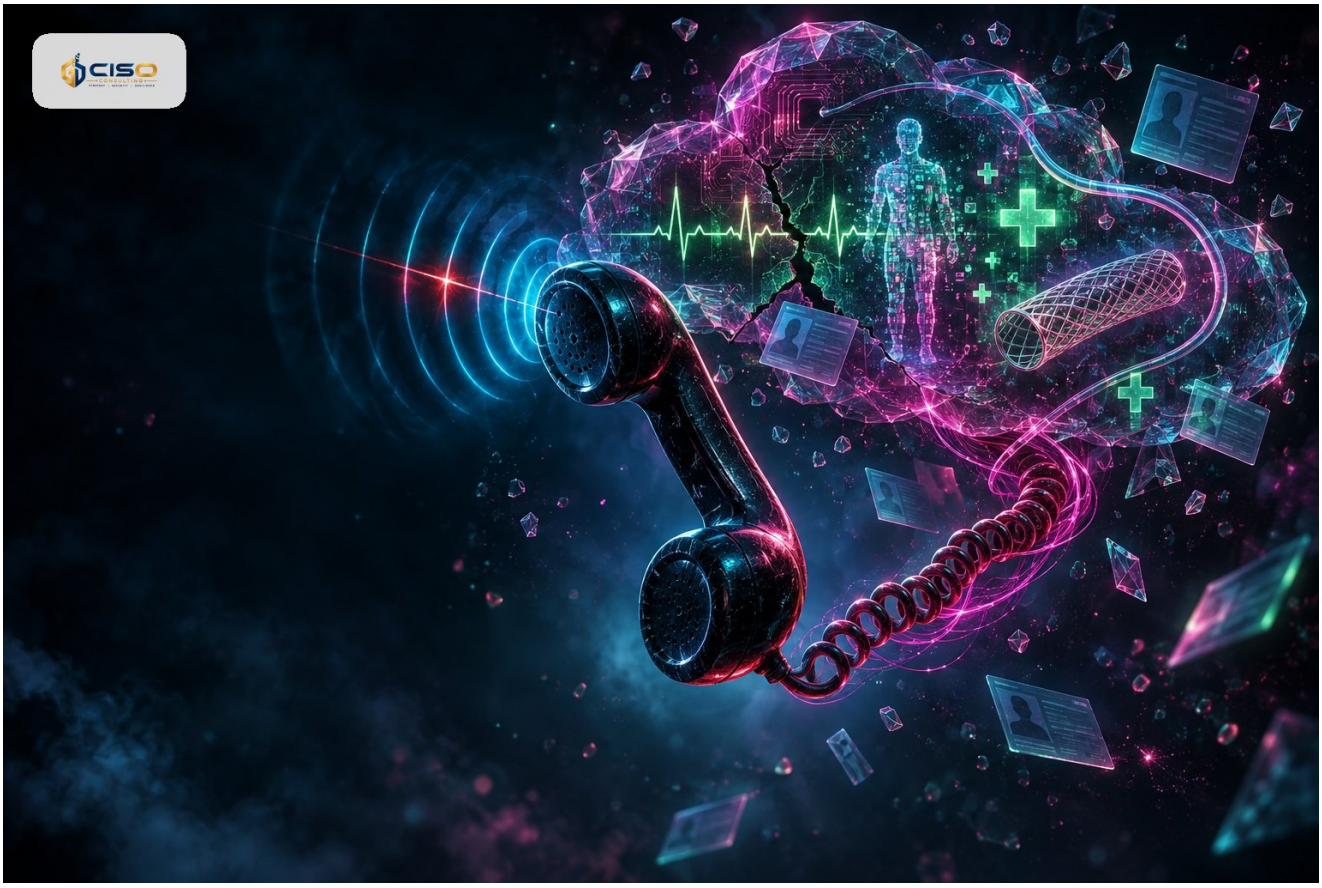
بوسطن ساينتفيك تؤكد اختراقًا سحابيًا عبر التصيد الصوتي كشف بيانات شخصية وطبية



تبلّغ بوسطن ساينتفيك المتضررين باختراق سحابي بدأ بهجوم تصيد صوتي. أفادت تكساس بتأثر 117,789 شخصًا، وتؤكد الشركة أنه لا علاقة له بحادثة أغسطس 2026.

- استخدم المهاجمون الهندسة الاجتماعية عبر التصيد الصوتي (vishing) للوصول إلى البنية السحابية للشركة.
- تذكر بوابة المدعي العام في تكساس تأثر 117,789 شخصًا، وشملت البيانات الأسماء والعناوين وأرقام الضمان الاجتماعي وأرقام الهويات الحكومية والمعلومات الطبية والتأمين الصحي وتواريخ الميلاد.
- وفق الإشعار، لم تتعرض السجلات الطبية للمرضى ولا بيانات المراقبة عن بُعد والأجهزة المتصلة وتطبيقات سير العمل السريري.
- تفيد الشركة بعدم حدوث تعطّل في التصنيع أو التوزيع أو الخدمة أو سلامة المنتجات.

- أكد متحدث باسم الشركة أن الحادثة لا علاقة لها باختراق أغسطس 2026 الذي بدأ عبر جهاز شبكي متصل بالإنترنت.

بدأت بوسطن ساينتفيك، الشركة الأمريكية المصنّعة للأجهزة الطبية، بإرسال إشعارات اختراق بعد هجوم سيبراني على بيئتها السحابية. ووفق نموذج إشعار قدمته الشركة إلى جهات أمريكية، استخدم المهاجم التصيد الصوتي للوصول إلى البنية السحابية، ما كشف تطبيقات سحابية وبيانات مستضافة فيها.

ما الذي انكشف

علمت الشركة بالوصول غير المصرّح به في 12 مايو، وخلص التحقيق إلى وقوع اختراق للبيانات في 5 نوفمبر. وتذكر بوابة الإبلاغ في تكساس أن عدد المتأثرين 117,789 شخصًا. وشملت البيانات الأسماء والعناوين وأرقام الضمان الاجتماعي وأرقام الهويات الحكومية والمعلومات الطبية ومعلومات التأمين الصحي وتواريخ الميلاد.

ويشير الإشعار إلى أن السجلات الطبية للمرضى وبيانات أنظمة المراقبة عن بُعد والأجهزة الطبية المتصلة وتطبيقات إدارة الحالات السريرية لم تتأثر. وتفيد الشركة بعدم حدوث تعطّل في التصنيع أو الطلبات أو التوزيع أو خدمة المرضى، ولا أثر على سلامة المنتجات.

السياق

هذه ثاني حادثة تعلنها الشركة في 2026. فقد تسببت حادثة أغسطس في انقطاعات وتعطّل تشغيلي عالمي، وخلصت CrowdStrike إلى أن المهاجم دخل عبر جهاز شبكي متصل بالإنترنت ولم تجد دليلاً على اختراق التطبيقات السحابية. وأكد متحدث باسم الشركة أن الحادثتين غير مرتبطتين، ورفض تقديم تفاصيل إضافية.

أهمية الخبر للجهات في المملكة

تبيّن الحالة أن اتصالاً هاتفيًا بأحد الموظفين قد يكفي للوصول إلى بيئات سحابية. وعلى الجهات التي تعتمد على موردي التقنية الطبية أو تحتفظ ببيانات صحية وهوياتية مراجعة آلية التحقق من الهوية في مكالمات الدعم، وكيفية إبلاغها عند وقوع حادثة لدى المورد.

ما يجب فعله الآن

1. اشترط تحققًا قويًا من الهوية يتجاوز البيانات الشخصية في طلبات مكتب المساعدة وإعادة تعيين كلمات المرور والمصادقة متعددة العوامل عبر الهاتف.
2. درّب الموظفين، ومنهم فرق الدعم والإدارة، على رصد التصيد الصوتي والإبلاغ عن المكالمات المشبوهة.
3. راجع الصلاحيات المميزة على التطبيقات السحابية ومخازن البيانات، وطبّق مصادقة متعددة العوامل مقاومة للتصيد حيثما أمكن.
4. تحقق من عقود موردي التقنية الطبية والخدمات السحابية فيما يخص مدد الإبلاغ عن الحوادث والتزامات حماية البيانات.
5. تأكد من أن إجراءات الإبلاغ عن الاختراقات وفق نظام حماية البيانات الشخصية (PDPL) تشمل الحوادث الناشئة لدى الموردين والمتعلقة بالبيانات الصحية والهوياتية.