تقارير عن هجوم فدية على جامعة فاندربيلت مرتبط بالأجهزة الشخصية BYOD



أفاد موقع BleepingComputer بتعرض جامعة فاندربيلت لهجوم فدية مرتبط بأجهزة BYOD مع ادعاء بسرقة بيانات. التفاصيل المتاحة محدودة، ويحسن اعتبار الخبر دافعًا لمراجعة ضوابط الأجهزة الشخصية.

- أُفيد بأن جامعة فاندربيلت تعرضت لهجوم فدية.
- وُصف الهجوم بأنه مرتبط بسياسة BYOD، أي باستخدام الأجهزة الشخصية.
- هناك ادعاء بسرقة بيانات، ولا تتوفر لدينا معلومات تؤكده.
- لم تتوفر تفاصيل تقنية إضافية في المادة التي اطلعنا عليها.

ما الذي ورد في الخبر

أفاد موقع BleepingComputer بأن جامعة فاندربيلت تعرضت لهجوم فدية مرتبط بسياسة BYOD، أي السماح للموظفين أو الطلاب باستخدام أجهزتهم الشخصية في العمل أو الدراسة. كما ذكر التقرير وجود ادعاء بسرقة بيانات.

لا تتضمن المادة التي اطلعنا عليها تفاصيل أخرى. لذلك لا يمكننا الجزم بكيفية ارتباط الأجهزة بالحادثة، ولا بما تأثر بها، ولا بمدى التحقق من ادعاء السرقة. ونكتفي بما ورد في العنوان دون استنتاجات إضافية.

أهمية الخبر للجهات في المملكة

تسمح جهات منظمة كثيرة في المملكة للأجهزة الشخصية بالوصول إلى البريد وأدوات التعاون والأنظمة الداخلية. وغالبًا ما تكون هذه الأجهزة أقل إحكامًا في الإدارة من أجهزة الجهة، ما قد يوسّع التعرض للفدية وتسريب البيانات. كما يذكّر الادعاء بالسرقة بأن حوادث الفدية الحديثة تثير مسائل حماية البيانات إلى جانب مسائل توافر الخدمة.

النهج المقترح

لا حاجة لإجراء عاجل بناءً على هذا التقرير وحده، لكنها فرصة مناسبة للتحقق من توافق ترتيبات BYOD لديكم مع مستوى المخاطر المقبول ومع متطلبات الهيئة الوطنية للأمن السيبراني والبنك المركزي السعودي ونظام حماية البيانات الشخصية. والإجراءات التالية ممارسات عامة جيدة وليست ردًا على تفاصيل مؤكدة للحادثة.

ما يجب فعله الآن

1. حصر الأجهزة الشخصية التي يمكنها الوصول إلى البريد والملفات والتطبيقات المؤسسية.
2. اشتراط تسجيل الجهاز والتشفير وتحديث الرقع قبل منح الوصول للأجهزة الشخصية.
3. تقييد ما تصل إليه الأجهزة الشخصية ومنع تخزين البيانات الحساسة محليًا عليها.
4. التأكد من وجود نسخ احتياطية معزولة ومُختبرة ومن تضمين سيناريوهات الفدية في خطة الاستجابة للحوادث.
5. تحديد آلية تقييم أي ادعاء بسرقة بيانات، بما في ذلك التزامات الإشعار وفق نظام حماية البيانات الشخصية.