Container Store تستعيد أنظمتها بعد هجوم سيبراني وسط ادعاءات مجموعة n0n

أعلنت Container Store استعادة موقعها وأنظمتها بعد حادث أثّر في الطلبات الإلكترونية ومعالجة المدفوعات في المتاجر. وكانت مجموعة n0n قد أدرجت الشركة على موقع التسريب، ولم تعلّق الشركة على ذلك.

- عطّل الحادث الطلبات الإلكترونية وألزم المتاجر باستخدام إجراءات بديلة لمعالجة المعاملات، مع بقائها مفتوحة.
- تقول الشركة الأم Neighborhood Intelligence إن الحادث اقتصر على The Container Store ولم يشمل علاماتها الأخرى.
- لا يبدو أن بيانات العملاء المالية سُرقت، لكن الشركة لم تتناول ادعاء n0n على موقع التسريب.
- ظهرت n0n في سبتمبر وتتخصص في الفدية وابتزاز البيانات، وتفيد التقارير بأنها هاجمت أكثر من 100 جهة.
- تفيد LevelBlue بأن المجموعة استعانت بأدوات ذكاء اصطناعي لكتابة نصوصها الهجومية وتصحيحها.

أعلنت Container Store، وهي شركة أمريكية لبيع مستلزمات التخزين المنزلي ولها نحو 100 متجر، أنها استعادت موقعها الإلكتروني وأنظمتها بعد حادث سيبراني وقع في عطلة الأسبوع السابق. وقد أوقف الحادث الطلبات الإلكترونية وقيّد معالجة المعاملات داخل المتاجر، وبقيت المتاجر مفتوحة عبر إجراءات بديلة.

ما هو معروف

تقول الشركة الأم Neighborhood Intelligence إن الحادث اقتصر على The Container Store ولم يشمل علاماتها التجارية الأخرى. وقد استعانت بخبراء في الأمن السيبراني لاحتواء الحادث واستعادة الأنظمة. ولا يبدو حتى الآن أن بيانات العملاء المالية سُرقت، غير أن الشركة لم تتناول ادعاءات مجموعة n0n التي أدرجتها على موقع التسريب في وقت سابق من الشهر.

عن مجموعة n0n

وفق المصدر، ظهرت n0n في سبتمبر وتتخصص في برمجيات الفدية وابتزاز البيانات، ويُقال إنها هاجمت أكثر من 100 جهة وطالبت بفديات بلغت مئات الملايين من الدولارات. وتفيد SOCradar بأن المجموعة انتقلت من فرض رسم قدره 10% للدخول إلى بوابة التفاوض إلى اشتراط دفع الفدية كاملة قبل عرض أي عينة من البيانات

المسروقة. ويقول Allan Liska من Recorded Future إن الشركات التابعة لها وُجّهت لاستهداف الشركات التي تتجاوز إيراداتها السنوية 10 ملايين دولار فقط. وتذكر LevelBlue أن المجموعة تستهدف أساساً الرعاية الصحية والأدوية، لكنها ادّعت مؤخراً امتلاك بيانات من شركات الخدمات المالية والتجزئة، وأنها تستخدم أدوات برمجة بالذكاء الاصطناعي لتوسيع عملياتها.

لماذا يهم ذلك

تُظهر الحالة أن حادث ابتزاز قد يعطّل المدفوعات والطلبات حتى مع استمرار البيع، وأن استعادة الأنظمة لا تحسم الأسئلة المتعلقة بالبيانات. وعلى الجهات المنظِّمة أن تستعد للعمل في ظروف متدهورة وأن تكون جاهزة لتقييم ادعاءات مواقع التسريب.

ما يجب فعله الآن

1. اختبار إجراءات بديلة أو يدوية للمدفوعات ومعالجة الطلبات لضمان استمرار الخدمات الأساسية عند تعطل الأنظمة.
2. وضع آلية للتحقق من ادعاءات ظهور المنشأة أو أحد مورديها على مواقع تسريب برمجيات الفدية وفرزها.
3. مراجعة خطط استمرارية الأعمال وفق متطلبات SAMA BCM وضوابط NCA ECC، بما في ذلك أهداف زمن استعادة أنظمة الدفع.
4. التأكد من حداثة عقود الاستجابة للحوادث ومسارات التصعيد إلى الجهات التنظيمية، ومنها التزامات الإبلاغ عن الاختراق في PDPL.
5. فحص التعرض عبر الأطراف الثالثة وشركاء التجزئة، والتأكد من تغطية البيانات لدى الموردين بشروط أمنية تعاقدية.