ماersk تؤكد اختراق بيانات عبر نظام قديم وجماعة WhiteArmor تطالب بفدية قدرها 5 ملايين دولار



أعلنت Maersk أن مهاجمًا وصل دون تصريح إلى نظام محلي قديم آل إليها عبر استحواذ سابق واستخرج بيانات منه. ويشير العنوان إلى مطالبة فدية بقيمة 5 ملايين دولار منسوبة إلى WhiteArmor.

- أكدت Maersk وقوع وصول غير مصرح به من جهة تهديد.
- النظام المتأثر نظام محلي قديم انتقل إليها عبر استحواذ سابق.
- استخرج المهاجم بيانات من هذا النظام.
- يربط العنوان الحادثة ببرمجية الفدية WhiteArmor ومطالبة بمبلغ 5 ملايين دولار.
- لا يوضح النص المتاح نوع البيانات أو عدد المتأثرين أو طريقة الاختراق.

ما الذي أُعلن

أكدت Maersk وقوع اختراق لبيانات. ووفق إعلان الشركة كما نقله موقع BleepingComputer، حصلت جهة تهديد على وصول غير مصرح به إلى نظام محلي قديم آل إلى الشركة عبر استحواذ سابق، واستخرجت منه بيانات. ويذكر عنوان المصدر أن مجموعة الفدية WhiteArmor تطالب بمبلغ 5 ملايين دولار.

ما لا يزال غير معروف

لا يبيّن النص المتاح لنا فئات البيانات المسروقة، ولا عدد الأفراد أو العملاء المتأثرين، ولا كيفية دخول المهاجم، ولا ما إذا تعطلت العمليات. وقد أبقينا هذه النقاط خارج الخبر بدل التخمين، ويحسن انتظار مزيد من الإفصاح قبل استخلاص نتائج.

أهمية الخبر للجهات المنظمة

تشير الحادثة إلى مخاطرة مألوفة: أنظمة تنتقل إلى المنشأة عبر الدمج أو الاستحواذ وتبقى خارج برنامج الأمن الأساسي. وغالبًا ما تكون المنصات القديمة أقل مراقبة وأقل انتظامًا في التحديث، فتصبح نقطة دخول أو مخزنًا للبيانات يسهل إغفاله. وعلى المؤسسات في المملكة التي استحوذت على كيانات أو ضمّت شركات تابعة أو أبقت أنظمة محلية قديمة أن تتحقق من التزام هذه الأصول بمستوى الضوابط نفسه المطبق في بيئتها الرئيسية، ومن الحاجة الفعلية إلى البيانات المخزنة عليها.

ما يجب فعله الآن

1. حصر الأنظمة القديمة والمستحوذ عليها، بما فيها المحلية، والتأكد من وجود مالك لكل نظام وإدراجه في سجل الأصول.
2. التحقق من شمول هذه الأنظمة بالمراقبة والتحديث وضبط الوصول والنسخ الاحتياطي بالمستوى نفسه المطبق على الأنظمة الأساسية.
3. مراجعة البيانات المخزنة على المنصات القديمة وأرشفة أو حذف ما لم تعد هناك حاجة إليه.
4. اختبار خطة الاستجابة للحوادث لتغطية سرقة البيانات المقترنة بالابتزاز، بما في ذلك قرارات التعامل مع طلبات الفدية وواجبات الإشعار وفق نظام حماية البيانات الشخصية.
5. إدراج العناية الواجبة الأمنية وجدولاً زمنيًا لدمج الأنظمة بعد الاستحواذ ضمن أي عملية دمج أو استحواذ.