أهولد ديلهايز تؤكد أن هجومًا سيبرانيًا عطّل خدمات متاجرها في أوروبا والولايات المتحدة



أكدت أهولد ديلهايز، إحدى أكبر شركات تجزئة الأغذية في العالم، أن هجومًا سيبرانيًا وقع الأسبوع الماضي عطّل خدمات في متاجرها بأوروبا والولايات المتحدة. ولا يورد المصدر تفاصيل إضافية.

- توصف أهولد ديلهايز بأنها من أكبر سلاسل تجزئة الأغذية في العالم.
- أكدت الشركة أن هجومًا سيبرانيًا وقع الأسبوع الماضي عطّل خدمات في متاجرها.
- شمل الأثر متاجر في أوروبا والولايات المتحدة.
- لا يوضح النص المتاح طريقة الهجوم أو أثره على البيانات أو حالة التعافي.

ما ورد في الخبر

أكدت أهولد ديلهايز، التي توصف بأنها من أكبر سلاسل تجزئة الأغذية في العالم، أن هجومًا سيبرانيًا وقع الأسبوع

الماضي عطّل خدمات في متاجرها عبر أوروبا والولايات المتحدة.

يقتصر النص المتاح لدينا على هذا التأكيد. فهو لا يبيّن كيف وصل المهاجمون إلى الأنظمة، ولا الأنظمة التي تأثرت، ولا ما إذا كانت بيانات قد سُرقت، ولا مدى استعادة الخدمات. لذلك لا نفترض شيئًا في هذه النقاط.

لماذا يهم المؤسسات في المملكة

تُظهر الحادثة أن هجومًا سيبرانيًا على شركة تجزئة قد يعطّل الخدمات في متاجر فعلية في عدة دول في وقت واحد. وتعتمد قطاعات التجزئة والخدمات اللوجستية والأنشطة الموجهة للمستهلكين في المملكة على أنظمة مترابطة مماثلة، ومن ثم فهي مناسبة لاختبار ترتيبات استمرارية الأعمال، لا مدعاة للقلق.

النهج المقترح

يمكن اعتبار الخبر تذكيرًا بمراجعة الجاهزية. راجعوا كيف ستستمر عملياتكم إذا تعذّرت أنظمة المتاجر أو الفروع أو نقاط الخدمة، وتأكدوا من معرفة متخذي القرار بمن يقود الاستجابة. تابعوا بيانات الشركة نفسها لمعرفة التفاصيل المؤكدة عند صدورها، وتجنبوا الاعتماد على تقارير غير موثقة.

ما يجب فعله الآن

1. مراجعة خطط استمرارية الأعمال لحالة فقدان أنظمة المتاجر أو الفروع أو نقاط الخدمة.
2. تأكيد وجود إجراءات يدوية أو بديلة للعمليات الرئيسية الموجهة للعملاء واختبارها.
3. التحقق من حداثة أدوار الاستجابة للحوادث ومسارات التصعيد ومن فهمها.
4. مراجعة فصل الأنظمة التشغيلية الحرجة عن شبكة تقنية المعلومات المؤسسية.
5. التأكد من حداثة النسخ الاحتياطية للأنظمة الرئيسية ومن اختبار استعادتها.