هجوم فدية يعطّل مجموعة مراكز بيانات IDCF Cloud في شرق اليابان



أعلنت IDC Frontier أن هجوم فدية استهدف خدمة IDCF Cloud وتسبب في انقطاع بمجموعة مراكز بيانات تخدم شرق اليابان. ولا تتضمن المادة المتاحة تفاصيل إضافية.

- توصف IDC Frontier بأنها شركة يابانية كبرى في الحوسبة السحابية والبنية الرقمية.
- أفادت الشركة بأن خدمة IDCF Cloud تعرضت لهجوم فدية.
- تسبب الهجوم في انقطاع بمجموعة مراكز بيانات تخدم الجزء الشرقي من اليابان.
- يشير عنوان الخبر إلى أن جهات حكومية تستخدم الخدمة.
- لا يتناول النص المتاح السبب أو أثر الهجوم على البيانات أو مدة الانقطاع أو التعافي.

ما الذي أُعلن

أفادت IDC Frontier، وهي شركة يابانية كبرى في الحوسبة السحابية والبنية الرقمية، بأن خدمة IDCF Cloud تعرضت لهجوم فدية. وأدى الحادث إلى انقطاع في مجموعة مراكز بيانات تخدم الجزء الشرقي من اليابان. ويشير عنوان الخبر إلى أن جهات حكومية تستخدم هذه الخدمة.

ما لا يزال غير معروف

النص المتاح لنا محدود، فهو لا يوضح كيف وصل المهاجمون إلى الأنظمة، ولا ما إذا كانت بيانات قد جرى الوصول إليها أو سرقتها، ولا مدة توقف الخدمات، ولا موعد استعادتها. لذلك لم نستنتج شيئًا في هذه النقاط، وينبغي انتظار بيانات لاحقة من مزود الخدمة.

الأهمية للمؤسسات في المملكة

تذكّر الحادثة بأن هجوم فدية على مزود خدمات سحابية أو استضافة قد يعطل خدمات عملاء كثيرين في وقت واحد، ومنهم جهات حكومية. وعلى المؤسسات التي تعتمد على خدمات سحابية من أطراف ثالثة أن تراجع مدى اعتمادها على مزود واحد أو موقع مركز بيانات واحد، وأن تتأكد من أن خطط استمرارية الأعمال تفترض تعطل المزود نفسه وليس الأنظمة الداخلية فقط.

لا يلزم إجراء محدد بسبب هذه الحادثة تحديدًا، لكنها مناسبة لمراجعة ترتيبات الأطراف الثالثة واستمرارية الأعمال القائمة.

ما يجب فعله الآن

1. حصر الخدمات الحرجة التي تعتمد على مزود سحابي واحد أو موقع مركز بيانات واحد.
2. التأكد من أن خطط استمرارية الأعمال والتعافي من الكوارث تغطي انقطاعًا مطولاً من جهة المزود.
3. مراجعة عقود مزودي الخدمات السحابية للتأكد من تحديد التزامات الإبلاغ عن الحوادث والتعافي.
4. التحقق من حفظ نسخ احتياطية للبيانات الحرجة بمعزل عن المزود الرئيسي واختبار استعادتها.