ديجيسيرت تعلن عن اختراق بيانات إثر خطأ في ترحيل الخوادم كشف نظامًا داخليًا



أفادت ديجيسيرت بأن خطأً أثناء ترحيل خادم جعل أحد أنظمة الأعمال الداخلية متاحًا عبر الإنترنت، ما أتاح وصولاً غير مصرح به إلى بيانات العملاء ووثائق الهوية.

- أعلنت ديجيسيرت عن اختراق بيانات طال معلومات العملاء ووثائق الهوية.
- تعود الحادثة إلى عملية ترحيل خادم عرّضت نظام أعمال داخليًا للإنترنت عن طريق الخطأ.
- تمكّن أطراف غير مصرح لها من الوصول إلى النظام المكشوف.
- لا يتضمن المقتطف المتاح من المصدر أرقامًا عن عدد العملاء المتأثرين.

حذّرت ديجيسيرت من تعرضها لاختراق بيانات. وبحسب التقرير، جرى تنفيذ عملية ترحيل خادم بصورة خاطئة، فبقي نظام أعمال داخلي مكشوفًا على الإنترنت، ما أتاح وصولاً غير مصرح به إلى معلومات العملاء ووثائق الهوية.

ما هو معلوم

النص المتاح من المصدر موجز. فهو يؤكد السبب (خطأ في الترحيل)، وطبيعة البيانات المكشوفة (معلومات العملاء ووثائق الهوية)، وأن الوصول كان غير مصرح به. ولا يورد هنا تفاصيل عن عدد العملاء المتأثرين أو الفترة الزمنية أو حقول البيانات المحددة.

الأهمية للجهات المنظَّمة

قد تكون الجهات في المملكة التي تشتري شهادات أو خدمات تحقق من ديجيسيرت قد قدّمت وثائق هوية أثناء التسجيل أو التحقق. وقد تتضمن هذه الوثائق بيانات شخصية، ولذلك فإن كشفًا لدى المورّد قد يرتب التزامات بموجب **نظام حماية البيانات الشخصية** ومتطلبات مخاطر الأطراف الخارجية، حتى لو كان الخطأ من جانب المورّد.

كما تبيّن الحادثة أن تغييرات البنية التقنية، مثل الترحيل، قد تفتح تعرضًا غير مقصود إذا لم تُراجع وفق خطوط الأساس الأمنية.

النهج المقترح

تجنّب الافتراضات إلى حين صدور إشعار مباشر من ديجيسيرت. تحقق مما إذا كانت جهتك متأثرة، وحدد البيانات التي شُورِكت مع المورّد، ووثّق تقييمك ليكون سندًا لأي نقاش تنظيمي لاحق.

ما يجب فعله الآن

1. تحقق مما إذا كانت جهتك تستخدم منتجات أو خدمات ديجيسيرت وحدد مالك الخدمة في الأعمال.
2. راجع وثائق الهوية والبيانات الشخصية التي قُدمت إلى ديجيسيرت لأغراض التحقق.
3. تابع إشعارات ديجيسيرت واطلب منها تفاصيل الحادثة مباشرة.
4. قيّم مع مسؤول حماية البيانات التزامات الإشعار وفق نظام حماية البيانات الشخصية عند تأكد الأثر.
5. أضف فحوصات مراجعة التعرض للإنترنت إلى إجراءات الترحيل والتغيير لديكم.