مجموعة GMO تدعو عملاءها إلى إيقاف أجهزتهم بعد اختراق خدمة Onamae Desktop Cloud



طلبت مجموعة GMO من عملائها فصل أنظمتهم عن الإنترنت وإيقاف أجهزتهم، بعد أن هدد مهاجم اخترق خدمة Onamae Desktop Cloud بشن هجوم فدية.

- طلبت GMO من عملائها فصل أنظمتهم عن الإنترنت وإيقاف تشغيل الأجهزة.
- يأتي التحذير بعد اختراق خدمة Onamae Desktop Cloud التابعة للشركة.
- هدد المهاجم بإطلاق هجوم فدية في يوم صدور الخبر.
- لا يتضمن المقتطف المتاح تفاصيل تقنية إضافية عن الاختراق أو نطاقه.

ما الذي أُعلن

دعت مجموعة GMO عملاءها إلى فصل أنظمتهم عن الإنترنت وإيقاف تشغيل أجهزتهم. جاء الطلب بعد أن هدد

مهاجم اخترق خدمة Onamae Desktop Cloud التابعة للشركة بشن هجوم فدية في يوم صدور الخبر.

ما لا يزال غير معروف

لا يوضح المقتطف المتاح كيف وقع الاختراق، ولا عدد العملاء المتأثرين، ولا المطالب التي طرحها المهاجم. لذا ينبغي التعامل مع الحادثة بوصفها قيد التطور، وعدم افتراض تفاصيل لم يؤكدها مزود الخدمة.

الصلة بالجهات في المملكة

تذكّر الحادثة بأن اختراق مزود خدمات سحابية أو سطح مكتب مستضاف قد يتحول سريعاً إلى خطر على العملاء المعتمدين عليه. وعلى الجهات في المملكة التي تستخدم خدمات سطح مكتب مستضافة أو وصولًا عن بُعد من أي مزود أن تعرف كيف ستتصرف إذا أصدر المزود تحذيراً مماثلًا، بما في ذلك من يملك صلاحية عزل الأنظمة وكيف تستمر الأعمال خلال ذلك.

لا يشير المصدر إلى تأثر جهات سعودية. وتكمن الفائدة العملية في مراجعة الجاهزية، لا في الاستجابة لهذه الحادثة تحديداً.

ما يجب فعله الآن

1. حصر خدمات سطح المكتب المستضاف والوصول عن بُعد والخدمات السحابية المقدمة من أطراف ثالثة، وتسجيل جهة الاتصال لدى كل مزود.
2. التأكد من تحديد من يملك صلاحية الأمر بعزل الأنظمة طارئاً ومن توثيق الإجراء.
3. التحقق من وجود نسخ احتياطية غير متصلة ومختبرة للأنظمة المعتمدة على خدمات يستضيفها المزود.
4. مراجعة خطط الاستجابة للحوادث واستمرارية الأعمال لسيناريو يحذّر فيه مزود الخدمة من هجوم فدية وشيك.
5. سؤال المزودين الحرجين عن آلية إبلاغكم عند وقوع اختراق وعن الإرشادات المؤقتة التي يقدمونها.