هجوم فدية على UNM Health يعطّل رعاية المرضى والعمليات الجراحية



أفاد تقرير بأن هجوم فدية على UNM Health عطّل رعاية المرضى والعمليات الجراحية. لم يتوفر سوى عنوان التقرير، لذا التفاصيل محدودة، وينبغي للجهات الصحية مراجعة جاهزيتها.

- تعرضت UNM Health لهجوم فدية بحسب BleepingComputer.
- شمل الأثر المعلن تعطل رعاية المرضى والعمليات الجراحية.
- النص المتاح لنا لم يكن مقروءًا سوى العنوان، ولذلك لا تتوفر تفاصيل مؤكدة أخرى.
- يعتمد العمل الصحي على استمرارية الأنظمة، ما يجعل الفدية مسألة تمس سلامة المرضى.

ما أُعلن

ذكر موقع BleepingComputer أن هجوم فدية استهدف UNM Health وأدى إلى تعطيل رعاية المرضى والعمليات

الجراحية. هذه هي المعلومة الوحيدة التي نستطيع تأكيدها، فنص التقرير لم يكن مقروءًا في المادة التي وصلتنا، ولذلك لا نذكر هوية المهاجمين ولا التاريخ ولا الأنظمة المتأثرة ولا حجم التعطل ولا حالة التعافي.

أهمية الخبر للمملكة

تعتمد المستشفيات والعيادات على السجلات الإلكترونية والمواعيد والتصوير الطبي والأجهزة الطبية. وعند تعطل هذه الأنظمة يتباطأ العمل السريري أو يتوقف، ويصل الأثر إلى المرضى مباشرة. وتواجه المنشآت الصحية في المملكة النوع نفسه من المخاطر، كما أنها تحتفظ ببيانات صحية شخصية حساسة تترتب عليها التزامات بموجب نظام حماية البيانات الشخصية.

خطوات عملية

يصلح هذا الحادث دافعًا لاختبار الجاهزية لا مدعاة للقلق. ينبغي للقيادات التأكد من أن الضوابط القائمة ستعمل فعلاً عند وقوع هجوم فدية حقيقي، وخاصة القدرة على مواصلة علاج المرضى أثناء تعطل الأنظمة الأساسية. وسنحدّث هذا الخبر إذا توفر عرض أكمل للحادثة.

ما يجب فعله الآن

1. اختبار إجراءات العمل أثناء تعطل الأنظمة (السجلات الورقية والجدولة اليدوية وتحويل الإجراءات) في الأقسام الحرجة.
2. التحقق من وجود نسخ احتياطية معزولة وغير قابلة للتعديل للأنظمة السريرية الرئيسية، وإجراء اختبار استعادة حديث.
3. مراجعة عزل الشبكات بين تقنية المعلومات الإدارية والأنظمة السريرية والأجهزة الطبية.
4. التأكد من أن خطة الاستجابة للحوادث تغطي الفدية، بما في ذلك صلاحيات القرار والتواصل مع الجهات التنظيمية والهيئة الوطنية للأمن السيبراني وتقييم الإبلاغ وفق نظام حماية البيانات الشخصية.
5. التحقق من تفعيل المصادقة متعددة العوامل للحسابات ذات الصلاحيات العالية وإحكام ضبط الوصول عن بُعد.