هجوم سيبراني على Crédit Mutuel Arkéa يتيح معاملات احتيالية تصل إلى 133 مليون دولار



تعرّض بنك Crédit Mutuel Arkéa التعاوني الفرنسي لهجوم سيبراني أتاح معاملات احتيالية تصل قيمتها إلى 133 مليون دولار، وردّ البنك بتعليق بعض أنظمته.

- استهدف الهجوم بنك Crédit Mutuel Arkéa التعاوني الفرنسي.
- أتاح الهجوم معاملات احتيالية تصل إلى 133 مليون دولار.
- علّق البنك بعض أنظمته استجابةً للحادثة.
- يشير عنوان الخبر إلى أن العملية تمت عبر مزوّد خدمات.

ما الذي أُعلن

تعرّض بنك Crédit Mutuel Arkéa، وهو بنك تعاوني فرنسي، لهجوم سيبراني أتاح تنفيذ معاملات احتيالية تصل

قيمتها إلى 133 مليون دولار. وبحسب التقرير، ردّ البنك بتعليق بعض أنظمته.

ويربط عنوان التقرير الحادثة بمزوّد خدمات. أما المقتطف المتاح لنا فلا يتضمن تفاصيل إضافية، ولذلك لا نتناول أسلوب الهجوم ولا المزوّد المعني ولا الإطار الزمني ولا استرداد الأموال.

أهمية الخبر للمؤسسات في المملكة

تذكّر الحادثة بأن انكشاف البنك يمتد إلى الأطراف الثالثة المرتبطة بعملياته المالية والتشغيلية. فحتى لو كان محيط المؤسسة نفسها محكماً، قد تصبح الصلاحيات الممنوحة لمزوّد خدمات طريقاً إلى معاملات احتيالية. كما أن تعليق الأنظمة خطوة احتواء معروفة، وتكون أكثر فاعلية عندما تكون مخططة ومجرّبة مسبقاً.

خطوات مقترحة

نقترح أن تستثمر فرق المخاطر والأمن هذا التقرير لمراجعة صلاحيات الأطراف الثالثة وضوابط المعاملات دون انتظار مزيد من التفاصيل. والإجراءات أدناه نقاط انطلاق عملية.

ما يجب فعله الآن

1. حصر مزوّدي الخدمات الذين لديهم وصول إلى أنظمة المدفوعات أو الأنظمة المصرفية الأساسية أو اعتماد المعاملات، والتأكد من الصلاحيات الممنوحة لكل منهم.
2. مراجعة صلاحيات المزوّدين وفق مبدأ الحد الأدنى من الصلاحيات، مع مصادقة قوية ومراقبة للجلسات.
3. التحقق من أن ضوابط كشف الاحتيال وحدود المعاملات ترصد التحويلات الكبيرة غير المعتادة، بما فيها ما يُبدأ عبر قنوات المزوّدين.
4. تجريب قرار تعليق الأنظمة، بما في ذلك من يملك صلاحية إقراره وكيفية استمرار الأعمال.
5. تأكيد التزامات الإبلاغ عن الحوادث في العقود مع المزوّدين واختبار مسار التصعيد، بما في ذلك إلى البنك المركزي السعودي عند الاقتضاء.