Cleverbridge تحذّر من اختراق طال أرقام البطاقات ورموز CVV



أفادت BleepingComputer بأن Cleverbridge حذّرت من أن مهاجمين سرقوا أرقام بطاقات ائتمان ورموز CVV في اختراق بيانات. على المؤسسات المتعاملة معها مراجعة تعرضها والاستعداد لمخاطر الاحتيال.

- حذّرت Cleverbridge من وقوع اختراق للبيانات.
- تشمل البيانات المسروقة بحسب التقرير أرقام بطاقات ائتمان ورموز CVV.
- لا يتضمن التقرير المتاح لنا تفاصيل مؤكدة إضافية عن النطاق أو التوقيت.
- على الجهات المرتبطة بـ Cleverbridge التأكد من تعرضها مباشرة مع الشركة.

ما الذي ورد في التقرير

تفيد BleepingComputer بأن Cleverbridge حذّرت من اختراق بيانات سرق فيه المهاجمون أرقام بطاقات ائتمان ورموز التحقق من البطاقة (CVV). والمهم هنا أن رقم البطاقة ورمز CVV سُرقا معًا، وهو المزيج الأكثر فائدة لعمليات الشراء الاحتيالية عبر الإنترنت.

ما لا نعرفه

لا تتضمن المادة المتاحة لنا تفاصيل مؤكدة أخرى، لذلك لا نذكر عدد المتضررين ولا توقيت الاختراق ولا طريقة دخول المهاجمين. وينبغي ألا يفترض القراء نطاقًا محددًا قبل أن تؤكده Cleverbridge أو التجار المتأثرون.

أهمية الخبر للمؤسسات المنظَّمة

تزيد بيانات البطاقات المقترنة برمز CVV من خطر الاحتيال في العمليات التي لا تتطلب حضور البطاقة. وبالنسبة للبنوك ومصدري البطاقات، قد يعني ذلك محاولات احتيال على بطاقات استُخدمت مع الخدمة المتأثرة. أما التجار وبائعو البرمجيات فيرتفع لديهم خطر الأطراف الثالثة وتبرز أسئلة الإبلاغ بموجب PCI DSS ونظام حماية البيانات الشخصية (PDPL).

الاستجابة المناسبة هادئة وعملية: تحديد ما إذا كانت مؤسستكم أو عملاؤكم مرتبطين بـ Cleverbridge، وجمع الحقائق من الإشعارات الرسمية، وتجهيز ضوابط مكافحة الاحتيال إلى حين اتضاح التفاصيل.

ما يجب فعله الآن

1. تحقق مما إذا كانت مؤسستكم أو منتجاتكم أو عملاؤكم يستخدمون Cleverbridge في المدفوعات أو المبيعات.
2. تواصلوا مع Cleverbridge أو مدير الحساب للحصول على إفادة رسمية عن تأثر بياناتكم من عدمه.
3. على مصدري البطاقات: تشديد مراقبة الاحتيال في العمليات دون حضور البطاقة والاستعداد لإعادة إصدارها عند تأكد التعرض.
4. راجعوا التزامات PCI DSS وواجبات الإشعار بموجب PDPL مع الشؤون القانونية والامتثال.
5. حدّثوا سجل مخاطر الأطراف الثالثة بهذه الحادثة ووثّقوا خطوات المتابعة.