تسرب بيانات متبرعين لمؤسسة كارنيغي للسلام الدولي عبر اختراق لدى مزوّد منصة جمع التبرعات



أفادت مؤسسة كارنيغي للسلام الدولي بأن هجومًا على مزوّدها Soapbox Engage كشف بيانات التواصل وسجل التبرعات لدى بعض المتبرعين، دون الكشف عن أرقام بطاقات كاملة.

- استهدف الهجوم منصة Soapbox Engage التي تستخدمها كارنيغي للتبرعات عبر الإنترنت، ووقع في 28 أكتوبر وأُخرج المهاجمون في 30 أكتوبر.
- شملت البيانات المسروقة الأسماء وعناوين البريد الإلكتروني وأرقام الهواتف وسجل التبرعات، ولم تُكشف أرقام بطاقات ائتمان كاملة.
- أتاح التكامل مع قاعدة بيانات كارنيغي للمهاجمين الوصول مؤقتًا إلى معلومات التواصل التي تحتفظ بها المؤسسة.
- أبلغت كارنيغي جميع الأشخاص في قاعدة بياناتها استنادًا إلى قوانين الخصوصية الأوروبية، واستعانت بشركة أمن سيبراني للتأكد من إخراج المهاجمين.

- لم يُعلن عدد المتضررين، كما أعلنت DonorPerfect وGoFundMe عن حوادث أمنية حديثة.

ما حدث

حذّرت مؤسسة كارنيغي للسلام الدولي متبرعين سابقين من أن بياناتهم تعرّضت للكشف إثر هجوم سيبراني على مزوّد خارجي هو Soapbox Engage، وهي منصة إلكترونية لجمع التبرعات وإدارة التفاعل مع الداعمين لدى المنظمات غير الربحية. وبحسب المؤسسة، وقع الحادث في 28 أكتوبر، وأُخرج المهاجمون من نظام المزوّد في 30 أكتوبر.

شملت البيانات المسروقة الأسماء وعناوين البريد الإلكتروني وأرقام الهواتف وسجل التبرعات. وتؤكد كارنيغي أن أرقام بطاقات الائتمان الكاملة لم تُكشف. وأوضحت متحدثة باسم المؤسسة أن التكامل مع قاعدة بيانات كارنيغي أتاح للمهاجمين الوصول مؤقتًا إلى معلومات التواصل التي تحتفظ بها، وأن نسبة صغيرة من القاعدة تأثرت. ولم يُعلن عدد المتضررين.

السياق الأوسع

أبلغت كارنيغي جميع الأشخاص في قاعدة بياناتها بسبب قوانين الخصوصية الأوروبية، واستعانت بشركة أمن سيبراني للتأكد من إخراج المهاجمين. ولم تردّ Soapbox Engage على طلبات التعليق. ويتزامن الحادث مع إعلانات من منصات تبرع أخرى؛ إذ أفصحت DonorPerfect عن حادث أمني، وأبلغت GoFundMe عن اختراقين منفصلين في أكتوبر ونوفمبر طالا بيانات شخصية محدودة. ونقلت The Nonprofit Times أن الهجمات بدت منسّقة.

الأهمية للمؤسسات في المملكة

يبيّن الحادث كيف يمكن للتكامل بين منصة المزوّد وقاعدة البيانات الداخلية أن يوسّع أثر اختراق المورّد. وتواجه المؤسسات في المملكة التي تستخدم منصات خارجية للتبرعات أو التفاعل مع العملاء أو إدارة العلاقات المخاطر نفسها، إضافة إلى التزاماتها بموجب نظام حماية البيانات الشخصية وتعليمات الجهات التنظيمية القطاعية.

ما يجب فعله الآن

1. حصر المنصات الخارجية المرتبطة بقواعد بيانات العملاء أو المتبرعين وتوثيق البيانات التي يمكن لكل منها قراءتها أو تعديلها.
2. تقييد حسابات التكامل ومفاتيح الربط البرمجي بالحد الأدنى من البيانات اللازمة، ومراجعتها وتدويرها دوريًا.
3. التأكد من أن عقود الموردين تلزمهم بالإبلاغ الفوري عن الحوادث ودعم التحقيق والاحتواء.
4. مراجعة إجراءات الإبلاغ عن الخروقات وفق نظام حماية البيانات الشخصية واختبارها على سيناريو حادث مصدره مورّد.
5. مراقبة نشاط التكامل لرصد الوصول غير المعتاد أو استخراج البيانات بكميات كبيرة، وتجهيز رسائل التواصل مع المتضررين مسبقًا.