مشرّعون أمريكيون يطالبون شركات التحقق من الهوية بتشديد حماية البيانات بعد اختراق IDScan



وجّه مشرّعون أمريكيون رسالة إلى شركات التحقق من الهوية بعد اختراق IDScan الذي كشف مسوحات لأكثر من 150 مليون وثيقة هوية، وطلبوا إيضاحات حول تخزين البيانات الحساسة وحمايتها.

- أدى اختراق في سبتمبر لمنصة IDScan السحابية إلى عرض مسوحات لأكثر من 150 مليون وثيقة هوية للبيع على الويب المظلم.
- طلب ستة مشرّعين من عدة شركات للتحقق من الهوية توضيح كيفية إدارة بيانات العملاء الحساسة وحمايتها.
- دعت الرسالة إلى البحث الاستباقي عن الثغرات واعتماد بنية انعدام الثقة والحد الأقصى الممكن من تقليل جمع البيانات الشخصية ومشاركتها وتخزينها.
- أفاد الصحفي Brian Krebs بأن أكثر من عشرين شركة من هذا النوع تخزّن مسوحات الهويات، غالباً بشكل افتراضي، وقد يدفع العملاء مقابلًا إضافياً لتجنب ذلك.

- أفاد Krebs بأن سرقة البيانات بدأت قبل أكثر من عام من العثور عليها على الإنترنت.

وجّهت مجموعة من ستة مشرّعين أمريكيين من الحزبين رسالة إلى عدة شركات للتحقق من الهوية بشأن ممارساتها الأمنية، عقب اختراق وقع في سبتمبر لدى IDScan. فقد سُرقت بيانات عملاء مخزّنة في المنصة السحابية للشركة، ثم عُرضت للبيع على الويب المظلم مسوحات لأكثر من 150 مليون رخصة قيادة ووثيقة هوية أخرى. ويجري مكتب التحقيقات الفيدرالي تحقيقاً في الحادثة.

ما الذي طلبه المشرّعون

تطلب الرسالة من الشركات إجابات تفصيلية عن كيفية تعاملها مع بيانات العملاء الحساسة وكيفية حمايتها من هجمات يزداد تمكينها بالذكاء الاصطناعي. وتحثها على البحث الاستباقي عن الثغرات، واعتماد بنية انعدام الثقة (zero-trust)، وتقليل جمع المعلومات الشخصية المعرِّفة ومشاركتها وتخزينها قدر الإمكان.

وتشير الرسالة الموجهة إلى الرئيس التنفيذي لـ IDScan إلى أن البيانات المكشوفة شملت، إلى جانب وثائق الهوية، نحو 600 ألف بطاقة طبية وتصاريح عمل وسجلات حساسة أخرى. وذُكر أن مسوحات الرخص تضمنت صوراً بالأشعة فوق البنفسجية وتحت الحمراء.

أهمية الحادثة خارج الولايات المتحدة

يقول الصحفي Brian Krebs، الذي كشف الاختراق أولًا، إنه وجد أكثر من عشرين شركة للتحقق من الهوية تخزّن مسوحات الهويات، غالباً بشكل افتراضي، وإن العملاء قد يضطرون إلى دفع مبلغ إضافي لإيقاف الاحتفاظ بها. ويضيف أن مجرمين على سوق Nexus بدأوا سحب البيانات قبل أكثر من عام من اكتشافها على الإنترنت.

لا يتناول المصدر أي أثر على المملكة. والدرس عام: المنشأة التي تسند التحقق من الهوية إلى طرف خارجي ترث مخاطر ما يحتفظ به مزوّد الخدمة، والاحتفاظ بصور الهويات خيار تصميمي يمكن التفاوض عليه والتحقق منه.

ما يجب فعله الآن

1. حصر مزوّدي الخدمة من الأطراف الثالثة الذين يجمعون مسوحات الهويات أو وثائق مشابهة أو يخزّنونها نيابة عن المنشأة.
2. سؤال كل مزوّد كتابياً عمّا إذا كانت المسوحات تُحفظ بعد التحقق، ولمدة كم، وكيفية تعطيل الاحتفاظ بها.
3. تضمين عقود الموردين بنوداً لتقليل البيانات وحدود الاحتفاظ وإثبات الحذف، بما يتوافق مع التزامات نظام حماية البيانات الشخصية.
4. مراجعة ضمانات الأمن لدى المزوّدين، بما يشمل ضوابط الوصول السحابي وإدارة الثغرات وممارسات انعدام الثقة.
5. تحديث خطط الاستجابة للحوادث لتغطي اختراق بيانات هوية العملاء لدى المزوّد، بما في ذلك خطوات الإبلاغ.