شركة كيبكو الكورية تؤكد اختراقًا طال نحو 1.5 مليون شخص



أعلنت شركة الكهرباء الكورية الحكومية كيبكو أن مهاجمًا خارجيًا سرق بيانات من بوابة العملاء ومنصة الموردين، بما فيها بيانات دفع، وهي مناسبة لمراجعة حماية البوابات وبيانات الأطراف الثالثة.

- أفصحت كيبكو عن اختراق طال نحو 1.5 مليون شخص، وشمل بوابة خدمة العملاء KEPCO ON ومنصة إدارة علاقات الموردين SRM.
- من بوابة KEPCO ON سُرقت بيانات 650,487 شخصًا، منها أرقام الهوية وبيانات الاتصال وتفاصيل البطاقات والحسابات البنكية وبيانات الفوترة.
- من منصة SRM سُرقت بيانات 869,761 فردًا، منها الأسماء وأرقام الهوية والبريد الإلكتروني وبيانات الاتصال بالشركات.
- لم تفصح كيبكو عن طريقة وصول المهاجم ولم تؤكد استخدام الذكاء الاصطناعي، وقد فتحت هيئة حماية المعلومات الشخصية الكورية (PIPC) تحقيقًا.

- علّقت الشركة الخدمات المتأثرة وحجبت الوصول الخارجي وأبلغت المتضررين والجهات المعنية.

أفصحت شركة الكهرباء الكورية (KEPCO)، وهي شركة حكومية في كوريا الجنوبية، عن اختراق لبيانات طال نحو 1.5 مليون شخص، وتنسبه الشركة إلى مهاجم خارجي.

ما الذي تأثر

شمل الحادث نظامين: بوابة خدمة العملاء المتكاملة KEPCO ON، ومنصة إدارة علاقات الموردين (SRM) المعنية بالمشتريات وعقود الخدمات. فمن KEPCO ON سُرقت بيانات 650,487 شخصًا، تضمنت الأسماء والعناوين وأرقام الهواتف وأرقام الهوية وأرقام العملاء وتفاصيل البطاقات والحسابات البنكية وبيانات الفوترة والدفع. ومن منصة SRM سُرقت بيانات 869,761 فردًا، شملت الأسماء وأرقام الهوية والبريد الإلكتروني وعناوين الشركات والأرقام الوظيفية وأرقام الهواتف، ومنهم موظفو كيبكو وموظفو شركات شريكة.

الاستجابة والأسئلة المفتوحة

تقول كيبكو إنها علّقت الخدمات المتأثرة فور اكتشاف الحادث، وحجبت الوصول الخارجي، وراجعت الأنظمة ونفّذت إجراءات المعالجة. وفي 20 نوفمبر أكدت حدوث تسريب فعلي للبيانات. وقد أبلغت المتضررين مباشرة والجهات المختصة، وستشارك تفاصيل انكشاف البيانات المالية مع جهات حكومية ومالية.

وجاء الإفصاح بعد منشور في 19 نوفمبر على منتدى في الشبكة المظلمة لمستخدم يحمل اسم Noiem، قيل إنه ادّعى امتلاك بيانات مستخدمين وموردين ووثائق مناقصات وعقود. وفتحت هيئة حماية المعلومات الشخصية الكورية (PIPC) تحقيقًا ولم تنسب الاختراق إلى هذا المستخدم. ولم تذكر كيبكو كيف حصل المهاجم على الوصول، ولم تؤكد استخدام الذكاء الاصطناعي، وإن أشارت إلى تزايد تعقيد الهجمات المعتمدة عليه.

لماذا يهمّ ذلك

تبيّن الحالة أن بوابات العملاء ومنصات الموردين قد تجمع بيانات الدفع والهوية والعقود في موضع واحد. ويمكن للجهات في المملكة التي تشغّل بوابات مماثلة أن تتخذها دافعًا لمراجعة انكشافها.

ما يجب فعله الآن

1. حصر بوابات العملاء ومنصات الموردين وتحديد البيانات الشخصية وبيانات الدفع والعقود المخزّنة في كل منها.
2. مراجعة ما إذا كانت بيانات البطاقات والحسابات البنكية محفوظة، وتقليلها أو ترميزها أو إخفاؤها كلما أمكن.
3. التحقق من ضوابط الوصول والسجلات والمراقبة على هذه المنصات، بما في ذلك مسارات الوصول الخارجي وتنبيهات تسريب البيانات.
4. التأكد من أن خطة الاستجابة للحوادث تغطي تعليق الخدمات وإبلاغ المتضررين وإشعار الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا) والجهة التنظيمية القطاعية وفق نظام حماية البيانات الشخصية.
5. رصد ما يُنشر في الشبكة المظلمة عن الجهة، وتحديد آلية للتحقق من عينات البيانات المزعومة.