Un ’hackeo’ a Endesa compromete el DNI y los datos bancarios de millones de clientes

Endesa confirma un acceso ilegal y posible robo de datos de clientes, entre ellos el DNI y los datos de IBAN de sus cuentas corrientes. Un portal especializado habla de más de 1 terabyte de datos robados de 20 millones de clientes

Endesa Energía ha reconocido un acceso no autorizado a su plataforma comercial que ha resultado en la extracción de datos de los clientes relacionados con sus contratos, incluidos el documento de identidad y los medios de pago.

Un actor malicioso ha sobrepasado las medidas de seguridad implementadas por la empresa en su plataforma comercial en un incidente de seguridad reciente, del que ya ha empezado a notificar a los usuarios afectados a través de un correo electrónico. Este incidente, un "acceso no autorizado e ilegítimo", como lo expone la compañía, ha resultado en la extracción de datos personales sensibles de los clientes relacionados con los contratos de luz y gas.

Según la investigación que ha iniciado la compañía, el actor malicioso "habría tenido acceso y podría haber exfiltrado" datos de contacto, documentos de identidad y el IBAN de la cuenta bancaria. Endesa Energía matiza que no se han visto afectadas las contraseñas de acceso.

Aunque por el momento no ha detectado un uso indebido de los datos robados, advierte de que el actor malicioso podría intentar usurpar o suplantar la identidad de los clientes, publicar dichos datos en foros digitales o utilizarlos para enviar correos o mensajes fraudulentos dentro de campañas de 'phishing' y de 'spam'. La compañía considera "improbable" que este robo "se materialice en una afectación de alto riesgo para sus derechos y libertades", aunque recomienda a los clientes que estén atentos a "posibles comunicaciones sospechosas que pudiera recibir en los próximos días" y les insta a comunicar cualquier acción sospechosa en el número de teléfono: 800 760 366.

Nada más conocer el incidente, Endesa Energía también ha activado los protocolos y procedimientos de seguridad establecidos para estos casos, así como "todas las medidas técnicas y organizativas necesarias para contenerlo, mitigar sus efectos y prevenir que se repita en el futuro". Especialistas de la firma de ciberseguridad ESET recuerdan que cuando una organización responsable de custodiar datos personales sufre un incidente de este tipo, el riesgo no termina con la notificación de la brecha. La información expuesta puede ser reutilizada durante meses, o incluso años, para lanzar fraudes, suplantaciones de identidad o ataques dirigidos que aprovechan la confianza de los clientes en la empresa afectada.

“Cuando se produce una filtración de datos, es normal sentir preocupación, pero también es importante mantener la calma y actuar con criterio. Los delincuentes suelen explotar estos incidentes haciéndose pasar por la empresa afectada, utilizando datos reales para ganar credibilidad y tratar de engañar a las víctimas”, explica Josep Albors, director de Investigación y Concienciación de ESET España. El portal 'Escudo Digital', que informó del 'hackeo' a Endesa el pasado 6 de enero, indicó de que el pirata informático que ha llevado a cabo el presunto ciberataque publicó detalles sobre el mismo en un foro de la 'dark web' el domingo 4 de enero, donde revelaba que se había hecho con más de 1 terabyte (TB) de información de la compañía referente a más de 20 millones de personas.

"Por los nombres de tablas y ficheros, el nivel de sensibilidad de los datos es extremo. Hay datos personales, como nombres y apellidos, datos de contacto, dirección postal, y relación cuenta-persona; datos financieros, como IBAN, datos de facturación e historial de cuentas y cambios; datos energéticos, como CUPS (identificador único de punto de suministro), contratos activos de luz y gas, datos del punto de suministro y datos regulatorios, como Listas Robinson, cuentas exentas e historial de incidencias", indicaba 'Escudo Digital'.

Fuente: https://www.elconfidencial.com/

LINK DE LA NOTICIA