

Hackeo al Banco Santander alerta sobre la ciberseguridad

Bases de datos. De clientes, funcionarios y exempleados en Chile, España y Uruguay fueron violadas desde un proveedor externo.

Marcelo González Cabezas

Con una pésima noticia, que se tradujo en obvia preocupación, se encontraron ayer los clientes del Banco Santander, la entidad de mayor tamaño en Chile en la medición de colocaciones, según datos de cierre de 2023 de la Comisión para el Mercado Financiero, con un 17,7% del total.

Desde la sede central en Madrid se informó en un comunicado que hubo "un acceso no autorizado a una base de datos de la entidad alojada en un proveedor", que afectó a usuarios de Chile, España y Uruguay, y también a todos los empleados y a algunos exempleados de la empresa.

Por ello fueron implementadas "medidas para gestionar el incidente, como el bloqueo del acceso a la base de datos y un refuerzo de la prevención contra el fraude para proteger a los clientes". Según la compañía, en tal base de datos "no hay información transaccional ni credenciales de acceso o contraseñas de banca por

CIFRA

165

Millones de clientes tiene el Banco Santander en Europa y América. En 2023 registró beneficios por 11.076 millones de euros.

internet que permitan operar con el banco. Las operaciones y los sistemas de Santander no están afectados y los clientes pueden seguir operando con seguridad".

El Grupo Santander notificó desde España esta situación a los reguladores y a las fuerzas de seguridad. También lamentó la situación y añadió que "estamos informando proactivamente a los clientes y empleados directamente afectados".

De acuerdo con Santander, que acá tiene casi cuatro millones de clientes y más de



El banco multinacional español es el de mayor tamaño en Chile. / AGENCIAUNO

2.500.000 cuentas corrientes, fueron robados datos personales, no datos operativos.

Pedro Huichalaf, del Centro de Investigación en Ciberseguridad de la Universidad Mayor, dice que "este ataque no fue dirigido a las instalaciones propias del banco, sino que a un proveedor externo que le

presta servicios y que mantenía algunas bases de datos. La institución tiene grandes medidas de seguridad, algo que quizás el proveedor no poseía", explica quien fue subsecretario de Telecomunicaciones durante el segundo periodo de la Presidenta Michelle Bachelet.

Huichalaf reseña que "las

bases de datos son unos de los objetivos más habituales de los delincuentes informáticos, quienes buscan acceder a datos clasificados, sensibles y personales, aprovechando todo tipo de brecha, como este el proveedor externo. Son usuales esta clase de ataques dirigidos".

El investigador de la Uni-



"Las bases de datos son unos de los objetivos más habituales de los delincuentes informáticos, quienes buscan datos clasificados, sensibles y personales".

PEDRO HUICHALAF
Universidad Mayor

versidad Mayor precisa que "esto no ocurrió en nuestro país, pero las empresas locales pueden verse afectadas por ataques como este... Chile tiene un margen de regulación sectorial a través de la Comisión para el Mercado Financiero, para los bancos, y de la Subtel, para las telecomunicaciones. Pero hay sectores sin estándares de seguridad exigibles, como el retail, por lo que son afectados por esta dinámica... Los clientes y usuarios siempre deben estar atentos y tener una cultura de ciberseguridad. Hay que dudar de todos los mensajes, pues los datos conseguidos ahora pueden ser usados de mala forma en un tiempo más para efectuar estafas caso a caso, suplantando los sitios del banco".