25/12/2024

7 incidentes de ciberseguridad que marcaron el 2024 en América Latina

Una selección de entre tantos ataques e incidentes de seguridad que afectaron a organizaciones en América Latina en 2024 para repasar las formas de ataque, la diversidad de organizaciones afectadas y el impacto que tuvieron las amenazas informáticas el úl

El 2024 fue un año en el que la ciberseguridad volvió a ser noticia. Así lo confirma el Banco Mundial: “América Latina y Caribe es la región de más rápido crecimiento en incidentes cibernéticos divulgados, con una tasa promedio de crecimiento anual del 25 % en la última década. Además, es la región menos protegida, con un puntaje promedio de ciberseguridad de 10,2 sobre 20”.

En este contexto, a continuación compartiremos una selección de incidentes de seguridad que afectaron a organizaciones en la región para dar un panorama del tipo de incidentes y perfil de los blancos afectados.

Si bien la lista podría ser mucho más extensa, con filtraciones y ataques de ransomware que afectaron a organismos de gobierno, entidades educativas y empresas de todo tipo de industrias en la región, el objetivo de este artículo es compartir casos reales y recientes para tener un panorama de lo que fueron las formas de ataque que más se observaron en América Latina durante 2024, así como los tipos de organizaciones o el impacto de los ataques.

Banco do Brasil

En marzo de 2024 se conoció el impacto del incidente de seguridad que tuvo como objetivo a uno de los bancos más importantes de Brasil. Puntualmente estuvo enfocado a los empleados de la entidad bancaria y permitió a los atacantes acceder a las bases de datos del banco. ¿El saldo? El robo de datos personales y financieros de más de 2 millones de clientes, que fueron usados para cometer delitos financieros por un total de 40 millones de reales.

Según informó la CNN, el grupo criminal contó con la colaboración directa del personal interno de la entidad financiera, que facilitaron la inserción de scripts maliciosos en los sistemas. De esta manera, los ciberdelincuentes obtuvieron el acceso remoto a los equipos del banco y, consecuentemente, de información sensible y confidencial.

En concreto, realizaron transacciones bancarias fraudulentas a nombre de clientes, alteraron los datos de registro y modificaron los datos biométricos de titulares de las cuentas. Ante este escenario, desde el Banco do Brasil se expresaron a través de la CNN: “Las investigaciones se iniciaron a partir de la investigación interna, que detectó irregularidades, que fueron comunicadas a las autoridades policiales. La normativa interna prevé soluciones administrativas que se pueden aplicar, que van desde la advertencia y suspensión hasta la desestimación de la posición y el despido”.

Gracias a la intervención de la Policía Civil del Río de Janeiro y el Ministerio Público del Río de Janeiro, bajo la operación “Llave Maestra”, se pudieron generar órdenes de allanamiento e incautación contra 11 de los sospechosos.

Interbank

En octubre de este año, una de las entidades financieras más conocidas de Perú sufrió una importante filtración de datos. Un actor

malicioso apodado kzoldiyck afirmó haber accedido a datos sensibles de clientes de Interbank, gracias al uso de credenciales internas que le permitieron acceder a servidores internos de la entidad administrados por terceros.

Concretamente, esta filtración del banco puso al descubierto datos personales de más de 3 millones de usuarios: nombres completos, números de tarjetas, teléfonos, fechas de nacimiento, documentos de identidad y hasta detalles de diversas transacciones bancarias.

La entidad confirmó que “un tercero” había accedido a cierta información con el objetivo de para extorsionarlos.

Luego del intercambio de varios mensajes entre el banco y el cibercriminal, y a sabiendas que la entidad no abonaría los 4 millones de dólares exigidos, el cibercriminal amenazó a la entidad asegurando que sufrirá las consecuencias de tal decisión.

Coppel

En abril de este año tuvo lugar un ciberataque que tuvo como víctima a la cadena mexicana de tiendas Coppel y que afectó a 1.800 tiendas en todo el país, que vieron diezmada su operatoria por un periodo de tres meses, según confirmó El Financiero.

Vale destacar que el saldo negativo de este periodo de inactividad (con cierres de sus tiendas en línea y la imposibilidad de procesar transacciones en sus tiendas físicas) significó para la empresa una pérdida cercana a los $15 millones de dólares en ingresos

Si bien la compañía no reveló cuál fue el origen ni el alcance real del ciberataque, medios como El Financiero se lo adjudican al grupo de ransomware Lockbit 3.0. Ante esto, Coppel afirmó en sus redes sociales que se activaron todos los protocolos de protección con el fin de poner al resguardo toda su información.

A su vez, Raúl Goycoolea, Chief Information Officer de Coppel, detalló: “En 2 meses y medio recuperamos y pusimos en funcionamiento el 86% de los servicios de negocio que se vieron afectados por el ciberataque, pero fue hasta después de 3 meses que logramos recuperar el 100% de nuestros servicios de negocio que teníamos limitados”.

Air-e

El 2 de septiembre de este año la empresa colombiana que distribuye y comercializa energía eléctrica en los departamentos de Atlántico, Magdalena y La Guajira sufrió un serio ataque de ransomware, el cual afectó sus sistemas y hasta dejó a los usuarios sin poder acceder a servicios como el pago de facturas a través de su sitio web.

Concretamente, Air-e encendió sus alarmas el 30 de agosto, cuando detectó una actividad inusual en sus sistemas. Ya durante el fin de semana, se evidenció un comportamiento anómalo, por lo cual debieron tomar medidas concretas y hasta realizar la denuncia ante la Fiscalía General de la Nación.

¿Las consecuencias para la empresa? No solo que su capacidad operativa de Air-e se vio afectada, sino que hubo retrasos en la atención de sus clientes, y hasta su gestión financiera y las operaciones logísticas quedaron paralizadas. A través de sus canales oficiales, Air-e emtió un comunicado para confirmar que los medios de pago de la empresa no se vieron afectados y continuaron siendo seguros en todo momento.

Consejería Jurídica del Poder Ejecutivo Federal (CJEF)

La Consejería Jurídica del Poder Ejecutivo Federal (CJEF) fue una de las víctimas del grupo RansomHub, ataque que tuvo lugar el 15 de noviembre y culminó con el secuestro de más de 300GB de información, entre contratos, presupuestos e información de sus funcionarios.

Como prueba del ataque, el grupo publicó un contrato de lineamientos para el alquiler de inmuebles utilizados por la Consejería Jurídica. La confirmación sobre este incidente llegó por parte de la propia presidenta mexicana, Claudia Sheinbaum, quien afirmó: “Me van a entregar un informe al respecto”.

Según detalla el medio El Informador, el grupo había dado plazo hasta el 25 de noviembre para que la institución pagara el rescato,

y sino la información recopilada sería liberada en la Deep Web. Como la entidad no efectuó el pago, el grupo liberó 206 GB de información.

Registro Nacional de las Personas

En abril de este año se publicaron en la plataforma de mensajería Telegram más de 100 mil fotografías de ciudadanos argentinos, que habían sido robadas en 2021 al organismo estatal encargado de la emisión de documentos de identidad y pasaportes en la Argentina, el Registro Nacional de las Personas, o RENAPER.

Si bien no se trata de un incidente de este año, la circulación en Telegram durante este año nos demostró cómo los datos que no pierden vigencia siguen circulando, incluso después de varios años de ocurrido un incidente. La filtración y publicación de estos datos ponen en riesgo a las personas ante ataques de phishing, de ingeniería social o incluso la suplantación de identidad.

Grupo Bimbo

En febrero surgió la noticia de que el Grupo Bimbo, empresa multinacional mexicana especializada en panificados y una de las más grandes del mundo, había sido víctima de un ataque de ransomware.

El grupo detrás del golpe es el ransomware Medusa, conocido por su capacidad de cifrar datos de los usuarios y añadir la extensión ". MEDUSA" a los archivos comprometidos. De hecho, el grupo no solo se atribuyó el ataque, sino que en su sitio web publicaron algunos archivos robados de la compañía como prueba.

En concreto, los ciberatacantes afirmaban tener en su poder bases de datos, datos financieros, facturas, correspondencia electrónica e información de empleados y clientes; y por eso exigían el pago de 6,5 millones de dólares como rescate.

Pensamientos finales

Estos casos reales de ataques vinculados a la seguridad de la información confirman la necesidad de que la ciberseguridad ocupe un rol estratégico en la agenda de las empresas y organizaciones de la región.

Ya sea por un ataque de ransomware o la filtración de datos, las consecuencias de estos incidentes pueden ser tan graves como irreversibles: desde el impacto monetario, a la exposición de datos sensibles y confidenciales, con la consecuente pérdida de confianza para con los clientes y/o usuarios.

Ante este escenario y ya con la mira puesta en el 2025, la adopción de medidas proactivas como la implementación de prácticas de seguridad robustas deben ser prioridad para así reducir sensiblemente la probabilidad de que un ataque sea exitoso.

Entre las principales acciones que deben contemplar las organizaciones, se destacan estar actualizadas con los últimos parches de seguridad, priorizar la educación continua del personal, e implementar de soluciones de respaldo y recuperación de datos efectivas.

Fuente: https://www.welivesecurity.com/

LINK DE LA NOTICIA