ÍNDICE DE INTELIGENCIA DE AMENAZAS X-FORCE DE IBM

Uno de cada cinco ciberataques, en contra de instituciones financieras

Fuga de datos financieros del cliente es una de las mayores amenazas que enfrentan las entidades financieras en México

José Soto y Rodrigo Riquelme
EL ECONOMISTA

LA INDUSTRIA financiera es víctima de 19% de los ataques cibernéticos en todo el mundo, de acuerdo con un análisis recién publicado por IBM. Esto significa que uno de cada cinco ataques a la confidencialidad, integridad y disponibilidad de la información se da en contra del sistema financiero.

En segundo lugar se encuentra la industria del transporte, con 13%, la cual incluye transporte aéreo, autobuses, ferrocarriles y transporte marítimo. Las empresas de servicios profesionales, es decir, aquellas que ofrecen servicios de consultoría en materia legal y contable figuran en el tercer lugar de la lista de las industrias que reciben más ataques, con 12%, mientras que las compañías de *retail* y manufactura también son afectadas.

De acuerdo con el Índice de Inteligencia de Amenazas X-Force de IBM, los siguientes sectores que más ataques cibernéticos reciben en todo el mundo son los de medios (8%), el gubernamental (8%), salud (6%), educación (6%) y energía (6 por ciento).

Los ataques a cajeros automáticos y las transferencias electrónicas fraudulentas, entre las mayores amenazas del sector financiero. FOTO: SHUTTERSOCK

70,000
EVENTOS
de seguridad por día, en 130 países, se monitorearon.

$300
MILLONES
se estima sumaron los ataques al SPEI en el 2018.

CAJEROS Y TRANSFERENCIAS, LOS MÁS AMENAZADOS

Las principales amenazas que enfrentan las instituciones financieras en México son los ataques a cajeros automáticos; las transferencias electrónicas fraudulentas a través de los sistemas SWIFT y Sistema de Pagos Electrónicos Interbancarios (SPEI) y las operaciones de compraventa de activos financieros, de acuerdo con Juan Carlos Carrillo, director de Servicios de Seguridad de IBM.

"Entre las mayores amenazas a las organizaciones financieras en México se encuentran los ataques a los cajeros automáticos, las transferencias electrónicas fraudulentas y las operaciones de compraventa de activos financieros", dijo Carrillo durante el Seminario de Ciberseguridad organizado por NYCE y SIGE en la Ciudad de México.

Según el especialista, la fuga de datos financieros del cliente es también otra de las mayores amenazas que enfrentan las entidades financieras en México.

Durante el 2018, el sistema financiero mexicano se vio afectado por una serie de ataques cibernéticos en contra de diversos bancos e instituciones financieras, entre los que destacan el Banco Nacional de Comercio Exterior, Banorte y varios más. Dichos ataques fueron ocasionados por vulneraciones a la infraestructura de conexión entre la plataforma SWIFT, el SPEI y varios participantes del sector, lo que ocasionó pérdidas calculadas en alrededor de 300 millones de pesos e interrupciones y retrasos en el uso de estos sistemas para realizar transferencias.

En octubre del 2018, la aseguradora AXA también fue víctima de un ciberataque en su conexión con el SPEI y hace apenas unas semanas CIBanco fue igualmente víctima de un ataque cibernético.

Juan Carlos Carrillo celebró la normativa diseñada por Banco de México tras los ataques al sistema de pagos SPEI del 2018, pero sugirió a los actores del sector financiero —y en general a todas las corporaciones que manejan sistemas informáticos— que construyan una cultura de monitoreo permanente de sus sistemas electrónicos.

Por el contrario, "los sectores más desprotegidos a ciberataques y brechas de seguridad de la información son los de salud, gobierno y educación", dijo el especialista de IBM a **El Economista**.

PHISHING POR CORREO ELECTRÓNICO SIGUE SIENDO EL REY

De acuerdo con el reporte de IBM, un tercio (29%) de los ataques analizados por la compañía está vinculado con compromisos a través de correos electrónicos de *phishing*, es decir, que buscan engañar al usuario del correo para que dé clic en un enlace y así tener acceso a su computadora o incluso a la red.

"De estos, 45% involucró estafas de compromiso de correo electrónico comercial (BEC), también conocidas como fraude de CEO o ataques de caza de ballenas. Cuando se trata de los tipos más lucrativos de estafas de ingeniería social, BEC ha sido una marea creciente durante varios años que abarca todas las industrias y geografías. Las estafas de BEC pretenden originarse en un propietario o CEO o un empleado de alto rango. Se envían a quienes controlan las cuentas bancarias de la empresa con instrucciones para realizar una transferencia bancaria confidencial", indicó el informe.

"Muchos de los ataques de *phishing* siguen siendo hacia correo corporativo, sí hay *phishing* contra correos personales, pero vemos un crecimiento importante de *phishing* a correos corporativos", expresó Carrillo.

IBM destacó en su reporte que casi un tercio (30%) de las vulnerabilidades documentadas por sus investigadores que han sido divulgadas en las últimas tres décadas ha sido reportado en los últimos tres años, lo que significa más de 42,000 vulnerabilidades, además menciona que la mitad de los ataques registrados en el 2018 fueron ataques nunca antes vistos.

El análisis de IBM es el resultado del monitoreo de datos a partir de 70,000 millones de eventos de seguridad por día en más de 130 países, junto con datos derivados de activos ajenos a sus clientes, como sensores de *spam* y redes. "Los investigadores de X-Force también ejecutan trampas de *spam* en todo el mundo y monitorean decenas de millones de ataques de *spam* y *phishing* a diario, analizando miles de millones de páginas web e imágenes para detectar actividades fraudulentas y abusos de marca para proteger a nuestros clientes", refirió la compañía.