Ciberseguridad en el sector financiero

Sin lugar a duda, la ciberseguridad es una de las cuestiones del panorama tecnológico actual que más está resonando en el ámbito económico y social del mundo desarrollado. Enfrentar los riesgos de ciberataques elevará los costes de operación, pero también ayudará a restaurar la confianza de los clientes.

Carlos Juarros Huerga | *Gerente de Ciberseguridad Mnemo Evolution & Integration Services S.A.*

Uno de los puntos de inflexión más claros en ciberseguridad fue el famoso **ciberataque Wannacry en 2017**, que afectó severamente a bancos, servicios sanitarios y redes de transporte de **más de 150 países**.

El **cibercrimen está cambiando el concepto que teníamos sobre la ciberdelincuencia** ya que ahora el cibercriminal puede estar a miles de kilómetros de nosotros. El campo de estudio conocido como «journey to crime» estudia los trayectos de los delincuentes para cometer sus fechorías. El investigador Andy Brumwell analizó los trayectos de casi 260.000 infractores, lo que ha permitido saber, por ejemplo, que existe una clara tendencia a delinquir a una distancia prudencial de sus viviendas (ni demasiado cerca, por si los reconocen, ni demasiado lejos, para que el gasto y el esfuerzo no sean elevados). La irrupción de internet ha posibilitado que los **delincuentes encuentren a sus víctimas, casi sin gasto y sin esfuerzo, a miles de kilómetros de distancia**, ampliando enormemente el mercado de víctimas potenciales.

Casos reales de ciberataques

Si acudimos a las estadísticas oficiales veremos que la cibercriminalidad no deja de crecer año tras año. Las estadísticas señalan que las tres industrias más atacadas en el mundo son, por orden, la banca, el *retail*, Gobierno y otros servicios, lo que posiciona al sector financiero como el principal objetivo de los ciberdelincuentes.

Existen ejemplos recientes como la cadena de ciberataques recibidos por el sistema bancario peruano en agosto de 2018. Como consecuencia, tuvieron que suspender temporalmente sus servicios al verse afectadas al menos seis entidades financieras.

Tampoco se puede olvidar que, en agosto de 2018, saltaron las alarmas en todo el mundo cuando se filtró un in-

forme interno del FBI dirigido a los bancos. El informe tenía como objetivo advertir a los bancos para que extremasen las precauciones y medidas de seguridad ante un posible ciberataque coordinado a cajeros automáticos de todo el mundo. La estrategia del robo consistía en sustraer millones de dólares clonando tarjetas bancarias.

Más cerca, y también en agosto de 2018, el **Banco de España sufrió un ciberataque** que llegó a materializarse y que impedía el acceso a su web desde servidores externos. A la vez, un equipo de investigadores de seguridad de IBM X-Force revelaba que el troyano bancario BackSwap (capaz de cambiar el número de cuenta del destinatario de las transferencias bancarias, así como robar las claves de acceso al banco de la víctima) tiene a nuestro país en el punto de mira, al detectarse que en la lista de objetivos de este *malware* se encuentran seis de los principales bancos españoles.

Cómo afecta al sector financiero

Estos últimos casos recuerdan que **el 40% de los ataques web están dirigidos a la obtención de información**, siendo las aplicaciones web patrocinadas por el sector público y el financiero las que mayor número de ataques reportaron en 2017.

Entre los **principales tipos de ataque** orientado que están sufriendo los mercados financieros se encuentran los siguientes:

- Accesos no autorizados a los sistemas financieros
- Corrupción de la información
- Interrupción de los sistemas
- Accesos no autorizados a las cuentas
- Manipulación de los límites de operación
- Propiciar errores en el cálculo de márgenes
- Borrado, modificación de registros de liquidación de órdenes
- Envío de información falsa mediante *spoofing* (suplantación de identidad)
- Manipulación de los algoritmos de cálculo de índices
- Manipulación de los protocolos de intercambio de información financiera
- Hackeo y control de los sistemas de *trading*

Contar con un **Programa de Ciberseguridad** provee a la organización de un instrumento para la gestión adecuada de la seguridad de sus activos de información que, alineado con la estrategia corporativa, **convierte a la seguridad en un habilitador de negocio** y genera la transformación del riesgo en oportunidades.

Medidas de protección para evitar ciberataques

Si bien las nuevas regulaciones para enfrentar los riesgos de ciberataques elevarán los costos de operación, también ayudarán a restaurar la confianza de los clientes. Por tanto, es importante disponer de un plan estratégico para recoger el análisis general de riesgos del sector financiero sobre las principales infraestructuras (incluidas las tecnológicas) e implantar **medidas de protección para prevenir, evitar y mitigar los ciberataques**:

- Desarrollar y evaluar un programa de seguridad de la información corporativa o transformar el existente.
- Identificar y gestionar las amenazas a las que se enfrenta el negocio.
- Aplicación de regulaciones, normas y estándares internacionales de seguridad de datos personales y privacidad, así como las tendencias tecnológicas como el cómputo en la nube.
- Elevar el nivel de la seguridad de la información a un nivel certificable bajo diferentes estándares internacionales
- Diseñar planes de continuidad de negocio y de recuperación de desastres, enfocado a los riesgos a los que se está expuesto.
- Administrar los accesos y las identidades de manera eficiente y efectiva.
- Proteger la confidencialidad, integridad y disponibilidad de los datos.
- Fomentar la educación y cultura de ciberseguridad entre los usuarios finales, y el personal de las propias instituciones que, a través de una capacitación continua, redunde en una participación activa para mitigar los riesgos de ciberataques.
- Colaborar en proyectos para fortalecer los controles de seguridad de los distintos componentes de las infraestructuras y plataformas operativas que soportan los servicios financieros, promoviendo el aprovechamiento de las tecnologías de información para prevenir, identificar, reaccionar, comunicar, tipificar y hacer un frente común ante las amenazas presentes y futuras.

Como dijo hace unos años **Gene Spafford**, destacado experto en seguridad informática: ***«En general, la gente no está interesada en pagar más por tener más seguridad. Al principio, los cinturones de seguridad costaban 200$ y nadie los compraba»***.

Esta ingeniosa frase nos hace recordar que, aunque el sector se encuentra cada vez más concienciado, las inversiones en ciberseguridad continúan siendo insuficientes existiendo una alta exposición al riesgo de los negocios del sector financiero. Asimismo, resulta fundamental la formación en la materia de todos los agentes involucrados.

Para conseguirlo, existen soluciones y compañías que nos ayudan a proteger nuestra información y cursos innovadores que nos permiten aprender a blindarnos ante los ciberdelincuentes o, lo que es lo mismo, hacer que ese cinturón de seguridad pase a ser un gran aliado para la continuidad del negocio.

En este contexto, el curso de especialización en Ciberseguridad y Ciberriesgos, que imparte Afi Escuela junto con MNEMO, compañía especializada en ciberseguridad, hace que los alumnos aprenden a controlar los principales riesgos a los que se expone la compañía y a generar estrategias en ciberseguridad ::