# Hackeo en Fintech:
# ¿cómo y por qué proteger a este sector?

CIUDAD DE MÉXICO. Octubre de 2022.- Los servicios que ofrecen las instituciones de tecnología financiera en la actualidad son sumamente relevantes y atraviesan un momento de crecimiento exponencial.

Tan solo el año pasado, el sector tuvo un crecimiento en México de 16% de acuerdo con un reporte de Finnovista y el Banco Interamericano de Desarrollo (BID). Estas empresas, que ofrecen soluciones de pagos digitales, préstamos, billeteras digitales, entre otras, incluso han llamado la atención de las instituciones financieras tradicionales.

Un estudio de KPMG señala que el 75% de esas empresas y de los bancos consideran que la colaboración es la mejor vía para generar beneficios, tanto para ambas partes como para el consumidor final.

Pero su exponencial crecimiento también implica una serie de riesgos para el sector, que debe estar alerta de las principales amenazas cibernéticas a nivel global. Se trata de empresas que operan con información sensible del usuario, y que al estar basadas 100% en plataformas digitales son potencialmente vulnerables.

- ¿Qué riesgos enfrentan?

Conforme los avances tecnológicos se aceleran, las amenazas cibernéticas para las *fintech* son mayores, ya que se vuelven más sofisticadas y requieren de herramientas de detección y mitigación más robustas.

Deloitte señala en un reporte que los niveles de vulnerabilidad de este tipo de compañías son elevados, lo que demanda de un constante estado de alerta particularmente en México que, según la consultora, presenta altos niveles de amenazas cibernéticas.

Una de las principales problemáticas que enfrentan las *fintech* es la exposición a determinadas amenazas como el *phishing*, robo de datos y el *ransomware*. El año pasado, por ejemplo, se registró un incremento de *phishing* a nivel global del 70% de acuerdo con un estudio realizado por Sophos. Además, el 66% de las organizaciones del mundo se vieron afectadas por *ransomware* el año pasado.

Otro problema que enfrentan las fintech son los riesgos de ser vulneradas en sus procesos de autenticación. Estas empresas no pueden darse el lujo de contar con procesos tradicionales que no impliquen herramientas multifactor y el uso de biométricos, como las huellas dactilares, el reconocimiento facial e incluso la voz, para la verificación de usuarios.

Por ello, Strike recomienda establecer un enfoque de ciberseguridad periódico que proteja a las *fintech* de las constantes y cambiantes amenazas que las acechan. Para ello se recomienda un *pentesting* continuo, que consiste en la revisión de los sistemas por parte de un *hacker* ético; es decir, un experto en vulnerabilidades que utiliza las mismas herramientas que un ciberdelincuente, pero con fines benignos para la detección de vulnerabilidades.

A diferencia de un escaneo tradicional, en el que las compañías tienen resultados hasta después de un mes y medio, el *pentesting* da muestra de las vulnerabilidades en menos de 24 horas, lo cual es fundamental en un sector que resguarda información financiera sensible y en el que se realizan millones de transacciones todos los días, las 24 horas del día.

Por la naturaleza de estas empresas, no es suficiente que se realice un *test* de este tipo y se crea que la compañía está completamente protegida. Por el contrario, el *pentesting* continuo significa que estas revisiones se llevan a cabo de forma frecuente, con una periodicidad establecida, buscando acompañar al ciclo de vida de desarrollo de software de la empresa.

El crecimiento de las *fintech* es importante en materia de innovación, inclusión financiera y digitalización de la economía, pero del mismo modo que se genera el crecimiento de estas compañías se deben crear estrategias en torno a protegerlas y cuidar la privacidad de los usuarios que las utilizan.

Hacer uso del *hacking* ético es fundamental para contar con soluciones ágiles que respondan a las necesidades de un sector de tan rápido crecimiento, a diferencia de las herramientas tradicionales que suelen ser excesivamente costosas, y que demoran tiempo en entregar resultados.

-o0o-

**Sobre Strike**

Strike es la plataforma de ciberseguridad en Latinoamérica. Su principal misión es ayudar a que las compañías estén protegidas a través de la detección y resolución de vulnerabilidades en sus sistemas. Esto se realiza a través de tests de penetración - o pentests - llevados a cabo por su red global de hackers éticos, conocidos como “Strikers”, una comunidad global que reúne a los mejores expertos de ciberseguridad con reconocimientos y certificaciones internacionales. Su objetivo es impulsar una cultura de ciberseguridad de calidad y accesible, en la que la misma sea parte del ciclo de vida de las empresas y no algo estanco o independiente. Más información en: https://strike.sh/

**Contacto para prensa México**
another
Ahtziri Rangel | PR Expert
+ 52 1 55 1395 6970
ahtziri.rangel@another.co