

La amenaza invisible: ciberataques y robo de información en las finanzas

Por Óscar Caballero



En la era digital, donde la tecnología y las finanzas están profundamente entrelazadas, la seguridad de la información se ha convertido en una prioridad absoluta. Los ciberataques y el robo de datos son las nuevas amenazas que acechan al mundo financiero, poniéndolo en una situación de vulnerabilidad; estos ataques no sólo tienen el potencial de causar pérdidas económicas significativas, sino que también pueden socavar la confianza de las personas en las instituciones financieras. Un ciberataque es cualquier intento malintencionado de acceder y dañar o destruir redes y sistemas informáticos. En el contexto financiero, los más comunes incluyen el phishing, el ransomware y el hacking. Los ciberdelincuentes utilizan técnicas avanzadas para infiltrarse en sistemas de pago, bases de datos de clientes y redes de transferencia de dinero, teniendo como principal objetivo robar información sensible como detalles de cuentas bancarias, números de tarjetas de crédito y datos personales,

entre otros, que posteriormente pueden vender en el mercado negro o utilizar para llevar a cabo otros delitos financieros.

Cabe señalar que el robo de información es particularmente devastador en este sector debido a la naturaleza sensible de los datos involucrados. Información de cuentas bancarias, historiales de transacciones y datos personales de clientes son oro puro para los delincuentes, ya que con esta información pueden cometer fraudes monetarios, desviar fondos y comprometer identidades, causando un daño a largo plazo a individuos e instituciones.

Un ejemplo relevante de lo anterior es el robo de información en tarjetas de crédito. Los ciberdelincuentes pueden clonar tarjetas y realizar compras fraudulentas, lo que no sólo afecta a los clientes, sino que también implica altos costos para las empresas emisoras y las compañías de seguros. En este contexto, otro escenario preocupante es el ataque a los servicios de banca en línea, donde los hackers pueden

transferir grandes sumas de dinero fuera de las cuentas comprometidas. Por lo tanto, la ciberseguridad no puede ser secundaria; debe formar parte integral de la estrategia de negocios en las finanzas. La razón es simple: la pérdida de confianza puede ser devastadora. Las instituciones financieras se basan en ella, por lo que, si se percibe que no son capaces de proteger la información de sus clientes, seguramente verán su relación erosionada.

Para protegerse contra las amenazas, las instituciones financieras deben adoptar una postura proactiva. Esto incluye la implementación de tecnologías avanzadas de ciberseguridad como el cifrado de datos, la autenticación multifactorial y el uso de inteligencia artificial (IA) para detectar actividades sospechosas. Además, la capacitación continua del personal será fundamental para reconocer y responder ante amenazas. Asimismo, las evaluaciones periódicas de seguridad, tanto propias como de terceros, y las pruebas de

penetración ayudan a identificar y mitigar vulnerabilidades antes de que puedan ser explotadas. Al respecto, la colaboración juega un papel fundamental, ya que compartir información sobre amenazas puede ayudar a fortalecer la resiliencia de la industria financiera. En conclusión, los ciberataques y el robo de información representan amenazas serias y crecientes para el mundo financiero, por lo que la ciberseguridad debe ser una prioridad máxima para proteger a instituciones y clientes. De igual forma, la implementación de medidas robustas y una cultura de seguridad son esenciales para mantener la confianza, así como para lograr la estabilidad necesaria en la economía mundial. Dicho en otras palabras, ignorar estas amenazas no es una opción; el futuro de las finanzas depende de nuestra capacidad para defendernos contra ellas.

*** Socio Líder de Asesoría en Ciberseguridad de KPMG México**