www.mexis.net

6 TENDENCIAS DE CIBERSEGURIDAD EN MÉXICO PARA 2025

mexis aggity

Los cibercriminales buscarán explotar vulnerabilidades en sistemas de pago, inteligencia artificial y ransomware, afectando a empresas y usuarios en México.

El panorama de la ciberseguridad evoluciona, con amenazas cada vez más sofisticadas que impactan a sectores críticos de la economía. Para México, donde los sectores financiero y de tecnología financiera (fintech) están en rápida expansión, entender las tendencias globales de ciberseguridad es clave para anticipar y mitigar riesgos.

1. Ataques dirigidos a bancos centrales y sistemas de banca abierta

Con el aumento de iniciativas como los sistemas de pago instantáneo y la banca abierta, los bancos centrales enfrentan un nuevo frente de ataque. En México, donde se discuten iniciativas similares a las vistas en otros países, como el sistema PIX de Brasil, las vulnerabilidades de las APIs utilizadas para compartir datos serán un blanco para los ciberdelincuentes.

Experto advirtió que **“el uso de estas tecnologías está abriendo nuevas ventanas de oportunidad para los cibercriminales,** particularmente en sistemas de pago electrónicos”.

Los ataques a APIs pueden permitir la manipulación de datos sensibles y el acceso no autorizado, algo que preocupa especialmente en un contexto donde las transferencias digitales son cada vez más comunes. Para 2025, se espera un aumento en los intentos de explotar estas vulnerabilidades, lo que podría impactar tanto a instituciones financieras como a usuarios finales.

2. Incremento en los ciberataques impulsados por inteligencia artificial

La inteligencia artificial (IA) ya está siendo utilizada para potenciar ataques, como el phishing y la suplantación de identidad, y en 2025 esta tendencia se intensificará. En México, donde las empresas están adoptando cada vez más sistemas de verificación biométrica para procesos de "know your customer" (KYC), **los ciberdelincuentes podrían emplear herramientas de IA para superar estas medidas.**

Por ejemplo, ya se han registrado casos internacionales en los que **herramientas basadas en IA manipulan imágenes y videos para crear identidades falsas** y abrir cuentas bancarias con fines de lavado de dinero.

“En cuanto más utilicemos estos sistemas, más abriremos la puerta a los atacantes”, dijo experto.

3. Proliferación del ransomware como servicio (RaaS)

El modelo de ransomware como servicio (RaaS) está facilitando que actores con poca experiencia técnica lancen ataques sofisticados. **En 2025, se espera un aumento en el uso de este modelo, particularmente contra pequeñas y medianas empresas mexicanas,** que a menudo carecen de medidas de seguridad robustas.

Además, **se prevé una diversificación en las tácticas de ransomware.** Por ejemplo, los atacantes podrían comenzar a modificar o insertar datos falsos en lugar de simplemente encriptarlos, dificultando la recuperación de información incluso después de pagar un rescate. **Esto podría tener un impacto devastador en sectores sensibles como el financiero, el de salud y el gubernamental.**

4. Crecimiento de los ataques a dispositivos móviles

México está experimentando un aumento en el uso de dispositivos móviles para transacciones financieras, y con ello, una expansión en las amenazas dirigidas a smartphones. **En 2024, los ataques a dispositivos móviles a nivel mundial se duplicaron en comparación con 2023, y se espera que esta tendencia continúe en 2025.**

Según Manjarrez, "la adopción tecnológica, aunque lenta por temas de resistencia al cambio y desconfianza, está en constante aumento", lo que también incrementa la exposición a amenazas digitales.

Los ciberdelincuentes están utilizando troyanos bancarios y aplicaciones fraudulentas que imitan transacciones legítimas para engañar a los usuarios. Esto es especialmente preocupante en un país donde el comercio electrónico y los pagos digitales están en auge. Para los consumidores mexicanos, las aplicaciones bancarias serán un punto crítico de vulnerabilidad.

5. Ataques a la cadena de suministro de código abierto

En 2025, se prevé un aumento en los ataques dirigidos a proyectos de código abierto, como lo demuestran incidentes recientes como el backdoor XZ. México, que está experimentando un crecimiento en el desarrollo de software y la adopción de tecnologías abiertas, no será inmune a este tipo de ataques.

Los ciberdelincuentes están aprovechando la confianza en repositorios de código abierto para insertar vulnerabilidades maliciosas que luego se propagan a múltiples proyectos. **Este tipo de ataques puede comprometer infraestructuras críticas y sistemas financieros si no se toman medidas preventivas.**

6. Auge de las amenazas basadas en blockchain y criptomonedas

El uso creciente de blockchain y criptomonedas en México está abriendo nuevas puertas para los ciberdelincuentes. **En 2025, se espera que surjan amenazas que aprovechen los protocolos descentralizados y el anonimato que ofrece esta tecnología.**

Además, la adopción de lenguajes de programación como Go y Rust para desarrollar malware vinculado a blockchain dificultará la detección y análisis de estas amenazas. Según la experta, **“más se va a abrir la puerta a nuevas amenazas”** con la implementación masiva de estas tecnologías, lo que subraya la necesidad de priorizar la seguridad desde su diseño.

Fuente de información:
eleconomista.com.mx