

COMUNICADO DE PRENSA

Auriga propone software de autoservicio avanzado y alerta sobre seguridad del ATM

1 de febrero de 2023.- Auriga, firma global desarrolladora de soluciones de software para la banca, continúa su expansión y propuesta tecnológica para México y la región latinoamericana con la exposición de las tendencias tecnológicas que destacarán durante 2024; en particular, sobre temas de autoservicio, inteligencia artificial y seguridad de los cajeros automáticos y sucursales automatizadas.

La desarrolladora propone la modernización de los servicios al cliente con software de autoservicio avanzado, al tiempo que observa y alerta sobre los riesgos para las instituciones financieras en tiempos de inseguridad, como ocurrió con el malware detectado en cajeros. Recién el año pasado se produjo el primer reporte de un nuevo *exploit* de *jackpotting* en cajeros automáticos en varios años en Latinoamérica: el malware bautizado como FiXS amenazó a los cajeros automáticos de la región latinoamericana, mayormente en México, con el objetivo de vaciar el depósito por completo. Por esta razón, para Auriga el tema de la ciberseguridad seguirá siendo un punto sensible durante 2024.

Auriga aconseja implementar estrategias de seguridad que partan del enfoque de confianza cero para los cajeros automáticos ante un posible ataque. Si bien FiXS es una variante de malware ATM nueva, las técnicas y tácticas que utiliza no son diferentes de las de otras familias de malware ya conocidas, como Ploutus, Tyupkin, Alice, Ripper o Cobalt.

En el caso de los cajeros automáticos, que deben estar accesibles por su propia naturaleza (fuera de las entidades o incluso de forma autónoma), los hace más vulnerables a ataques, tanto físicos como cibernéticos. Este canal de servicio es el ejemplo más antiguo y exitoso de tecnología financiera que existe, pero la falta de actualización de la mayor parte de los que hay en activo es un problema que los hace vulnerables y que las instituciones bancarias deben trabajar para resolver.

Bajo esta necesidad, [Auriga](#) presentó mejoras para su solución de ciberseguridad Lookwise Device Manager (LDM), con el objetivo de aumentar su capacidad de hacer frente a los ciberataques cada vez más sofisticados que están apareciendo en el sector.

El modelo Zero Trust consiste en asumir que la infraestructura que gestiona los cajeros y dispositivos de autoservicio asistido es vulnerable. Por ejemplo, que la imagen de software instalada en el ATM puede estar comprometida incluso antes de ser instalada, que el sistema de acceso remoto puede ser manipulado, que los técnicos de mantenimiento pueden no tener la seguridad en el ATM como su prioridad o que los atacantes pueden encontrar útiles los procesos de actualización de software para introducir malware.

Basándose en este modelo, la nueva versión de LDM mejora las funcionalidades de protección de las comunicaciones, centrándose en garantizar la seguridad de los procesos del ATM que necesitan acceder a la red. De este modo, al permitir solo conexiones fiables, los dispositivos están protegidos frente a ataques de acceso remoto o infecciones desde

dispositivos de red o fuentes no confiables. Además, Auriga ha ampliado las funcionalidades de encriptado para garantizar que incluso los modelos sin los módulos de almacenamiento de claves criptográficas (TPM) están protegidos, respondiendo así a las necesidades de más clientes.

En el más reciente reporte del Banco de México se contabiliza la operación de más de 60 mil cajeros automáticos de sucursal e individuales a lo largo del territorio nacional, los cuales han sido modernizados en los últimos años para, además de ser expendedores de efectivo, ofrecer soluciones de pagos, depósitos y otros servicios. Los especialistas de Auriga observan que la evolución se encamina para que el protagonista sea una terminal de autoservicio avanzado, un cajero evolucionado y mejorado con la incorporación de soluciones de gestión remota a través de audio y video.

“Un salto de calidad para el cliente y un salto de eficiencia (y rentabilidad) para la institución bancaria, ya que estas terminales pueden funcionar como oficinas independientes (hubs bancarios) o dentro de la sucursal tradicional, que también se transforma y se convierte en un espacio más versátil y con más opciones de atención, al que mismo tiempo que permite a la banca maximizar sus recursos”, explican los expertos de Auriga.