NOTA DE PRENSA

Auriga: la banca omnicanal debe invertir en estas tres claves de ciberseguridad

Ciudad de México a 25 de junio de 2021. Auriga, empresa especializada en soluciones bancarias omnicanal, dio a conocer las principales claves para prevenir y mitigar ciberataques en sucursales bancarias, ya que la pandemia aceleró la transformación digital y los ciberdelincuentes buscan lucrar con ella.

Según la Asociación de Bancos de México (ABM), el sector invirtió 20 mil millones de pesos en ciberseguridad, atención y prevención de fraudes el año pasado y prevé mantener esta cifra en 2021. Sin embargo los ataques a cajeros automáticos, el fraude a través de sitios falsos, la fuga de datos sensibles y el ransomware siguen en aumento.

De acuerdo con el Senado de la República, durante el primer semestre de 2020, se registraron 3 mil 100 millones de intentos de ciberataques a empresas, instituciones financieras y gubernamentales, derivado de las medidas de confinamiento y el trabajo a distancia.

A pesar de que el sector lleva años invirtiendo en ciberseguridad, los estudios más recientes muestran que sigue siendo un desafío poder identificar y estar a la altura de las ciberamenazas actuales, debido al número y complejidad de su evolución.

Por otro lado, el estudio de ciberseguridad Estado del Riesgo Cibernético en Latinoamérica en Tiempos del COVID-19, elaborado por Microsoft y Marsh, señala que más del 30 por ciento de las empresas latinoamericanas percibió un aumento de ataques cibernéticos como consecuencia de la pandemia, siendo el phishing la principal ciberamenaza. Por sectores, la industria financiera ha sido la más afectada y el 52 por ciento nota que hubo un incremento en incidentes de seguridad.

Claves para prevenir ciberataques en banca física

1. Uso de la inteligencia artificial (AI) y machine learning: Son herramientas que desempeñan un papel cada vez más importante en la ciberseguridad. A través de ellas se analizan datos de millones de incidentes cibernéticos y se utilizan para identificar amenazas potenciales. Por ejemplo, pueden detectar cuando una cuenta de empleado actúa de manera extraña al hacer clic en enlaces de phishing o una nueva variante de malware, y trabaja para detener el ataque.

El objetivo de la AI es identificar y reaccionar ante los problemas sospechosos casi de inmediato, a fin de evitar que los problemas potenciales interrumpan las actividades de los bancos y así poder garantizar que la red sea segura. Sin embargo, aunque la ciberseguridad basada en IA tiene muchos beneficios debe ser un complemento junto con el personal de seguridad humana, a fin de obtener mejores resultados ante los ciberataques.

2. Protección a cajeros automáticos: Dentro de las sucursales físicas el canal más propenso a los ataques cibernéticos son los cajeros automáticos, debido a que la mayoría funcionan con versiones de Windows de hace una década, están expuestos 24/7 y contienen dinero e información de los usuarios, por lo que son la lotería de los delincuentes. De acuerdo con el Banco de México, cerca de 282

millones de pesos se vieron afectados por el ataque a cajeros automáticos, y fue uno de los principales incidentes cibernéticos ocurridos en 2019.

Por ello, es de vital importancia que los bancos protejan la red de cajeros automáticos con soluciones que puedan monitorizar en tiempo real sus actividades y a partir de ello, los bancos tendrán una mejor imagen y la experiencia bancaria omnicanal de los consumidores se verá beneficiada.

3. Implementación de dispositivos de autoservicio dirigidos: Serán la interfaz entre el cliente y el banco del futuro, es decir, brindarán un mejor servicio al cliente a través de la banca física digitalizada. Por ejemplo, Bank4Me de Auriga es una solución avanzada de banca a distancia, diseñada para que los clientes tengan una atención más personalizada y puedan acceder a todos los servicios de las sucursales bancarias en modo autoservicio e interactuar con sus asesores a través de la asistencia por video de forma segura y personalizada.

Estos dispositivos deben estar suficientemente protegidos para ganarse la confianza de los clientes, ya que la seguridad es el elemento que puede convertirse en un diferenciador importante frente a otros canales, como el online o el móvil. Las instituciones financieras tendrán que analizar a fondo la ciberseguridad y las soluciones correspondientes este año y trabajar activamente para garantizar que tanto los datos personales de sus clientes como sus sistemas estén protegidos.

Soluciones integrales para la seguridad de los dispositivos

Cualquier solución de seguridad debe incluir los siguientes elementos: antivirus, prevención de copias de seguridad, firewalls, mantenimiento y monitoreo remotos. Un ejemplo de estas soluciones integrales es Lookwise Device Manager (LDM) de Auriga la cual permite a los equipos de seguridad bancaria monitorear el estado de seguridad de la red bancaria desde una única interfaz gráfica, evitando la necesidad de administrar múltiples soluciones independientes.

"*El LDM es una solución de seguridad integrada de múltiples proveedores que proporciona el modelo de protección en capas más avanzado para dispositivos de autoservicio, lo que permite monitorear el estado del sistema operativo o expansiones para servicios financieros (XFS, por sus siglas en inglés) y los eventos de seguridad relevantes*", explicó Rosvanna D´amico, ingeniera de producto en Auriga. "*El administrador trabaja agregando una capa de control adicional para que los equipos de operaciones puedan administrar el proceso de carga de claves y ejecutar acciones personalizadas remotamente para investigar o reaccionar a la nueva generación de ataques lógicos y físicos basados en malware*", señaló D´Amico.

Acerca de Auriga

Auriga es un proveedor líder de *software* y soluciones técnicas para las industrias bancarias y de pago, así como un proveedor especializado en soluciones omnicanal innovadoras para bancos y otras instituciones financieras. Sus soluciones, implementadas en más de un 70 % de los ATMs de Italia, se basan en arquitectura moderna y mejoran el tiempo de comercialización de los nuevos servicios, a la vez que reducen los costes, protegen los dispositivos críticos de los ciberataques y crean una ventaja competitiva a largo plazo. Auriga es una compañía global con presencia directa en Italia, Reino Unido, Francia, España, Alemania y México, y con operaciones en expansión en Europa Occidental y Oriental, Latinoamérica (LATAM) y Asia-Pacífico (APAC).

Visita www.aurigaspa.com/es/

Para más información:
Entercomm Latam
auriga@entercommla.com

Contacto con Auriga
Antonella Comes, directora de Marketing
antonella.comes@aurigaspa.com
Tel.: +39 080 56 92 255