# Ciberseguridad: una apuesta obligatoria para la banca

Con el creciente uso de las plataformas de banca digital y la sofisticación de los ciberataques, la inversión en ciberseguridad es actualmente uno de los ejes estratégicos para las entidades bancarias

**Madrid, 5 de mayo de 2021-.** Si algo ha impulsado la pandemia en términos de prestación de servicios han sido los canales digitales. Este proceso se ha vivido en todos los sectores y con especial intensidad en el financiero, lo que ha conllevado un aumento en los ciberataques tanto a entidades como a usuarios y ha generado pérdidas de millones de euros. Y es que, a medida que evolucionan los canales de acceso a la banca, también lo hacen las técnicas empleadas por los ciberdelincuentes. Por eso, en materia de seguridad, es importante ser activos en la detección de puntos débiles dentro del sistema para poder atajar cualquier futuro problema.

En cuanto a canales *online*, la banca digital ha sido uno de los objetivos principales de estos ataques. Por su parte, el eslabón más débil en los canales físicos continúa siendo el cajero automático o ATM. A pesar de tratarse de un canal muy valorado por los consumidores y que permite el acceso al efectivo en las poblaciones rurales, los cajeros automáticos no suelen incluirse en los programas de innovación de las entidades. Esto se debe a que tanto su *software* como su *hardware* son muy complejos y específicos, lo que dificulta el proceso de actualización y eleva su coste.

Además, deben estar disponibles las 24 horas, los 7 días de la semana, lo que reduce mucho el tiempo disponible para realizar las pruebas y actualizaciones necesarias. Así, a menudo nos encontramos con sistemas operativos obsoletos y sin parches que suponen una brecha en la seguridad del sistema y, por tanto, la puerta de entrada a los ciberdelincuentes. La conexión de varios ATMs en red permite la explotación de múltiples dispositivos de forma simultánea, lo que hace que estos ataques sean relativamente sencillos y muy rentables.

Pero no solo los ATMs suponen una gran vulnerabilidad para las entidades, también los nuevos dispositivos de autoservicio pueden presentar las mismas debilidades si no se interpone un sistema de seguridad eficiente. Son accesibles de forma física y dependen de las comunicaciones remotas y de la interconexión con la infraestructura de TI.

La prioridad en ambos casos es implementar una estrategia de ciberseguridad de Tecnología de Operaciones (OT por sus siglas en inglés) eficaz y conseguir una

completa monitorización del sistema, control remoto y en tiempo real para poder subsanar cualquier incidente. Lookwise Device Manager (LDM) es la solución integral de Auriga, proveedor líder de *software* y soluciones técnicas para las industrias bancarias y de pago, para la protección de los dispositivos físicos de las entidades bancarias. Permite monitorizar el estado de la red desde una única interfaz gráfica y ejecutarse en una red completa de forma remota. Genera varias capas de protección que atienden a la integridad de los archivos, listas blancas de aplicaciones, cifrado completo del disco y protección del *hardware*.

*Según Élida Policastro, vicepresidenta regional del área de Ciberseguridad de Auriga, "LDM proporciona el modelo de protección por capas más avanzado para los dispositivos de autoservicio, permitiendo supervisar el estado del sistema operativo o XFS y los eventos de seguridad relevantes".*

LDM permite gestionar los procesos de seguridad y supervisión de los dispositivos de la sucursal de una forma sencilla y centralizada y ofrece una protección ante distintos tipos de ataques, evitando cualquier comunicación de un agente externo para introducir *malware. "El gestor funciona añadiendo una capa de control adicional para que los equipos de operaciones puedan gestionar el proceso de carga remota de llaves y ejecutar acciones remotas personalizadas para investigar o reaccionar ante la nueva generación de ataques lógicos y físicos basados en malware",* añade Élida.

La inversión en ciberseguridad y en tecnología deben ir siempre parejas. Por un lado, si una entidad mantiene sus dispositivos desactualizados, se expone a que las avanzadas técnicas de ciberdelincuencia accedan a sus sistemas. Por otro, si efectivamente se decide invertir en una tecnología más potente, es necesario mantener unos altos estándares de seguridad, ya que a medida que la sucursal se digitaliza, se abren nuevos caminos para la explotación de las vulnerabilidades de sus sistemas.

**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 y crean una ventaja competitiva a largo plazo. Auriga es una compañía global que ofrece soluciones de transformación de bancos minoristas a nivel mundial.

**Para más información:**

Verónica Rodríguez veronica.rodriguez@alephcom.es
Jennifer Arenas jennifer.arenas@alephcom.es
Aleph Comunicación
Tel.: 91 386 69 99

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