CIBERSEGURIDAD PARA LA PRÓXIMA GENERACIÓN DE SUCURSALES BANCARIAS

MANTENER LA RED DE SERVICIOS DIGITALES ABIERTA Y SEGURA

ARTÍCULO DE OPINIÓN

AURIGA
the banking e-volution

THE # NEXTGENBANK®

www.aurigaspa.com

La pandemia de la Covid-19 ha acelerado la transformación tecnológica; todos nos hemos visto reconducidos hacia todo aquello que nos da acceso remoto. Esto incluye la tendencia de realizar transacciones digitales, algo que los ciberdelincuentes buscan explotar activamente.

Ahora que los servicios digitales se han adoptado ampliamente, la importancia de la ciberseguridad bancaria ha cobrado un nuevo impulso. Existe una necesidad imperiosa de tener todos los ángulos cubiertos y poder proteger preventivamente a los consumidores, sin importar qué canal estén usando. Se necesitan nuevos procesos y barreras para prevenir y mitigar los ataques.

Por tanto, es importante mirar la banca y la ciberseguridad desde diferentes perspectivas.

El ecosistema de los ATMs es vulnerable debido a su complejidad y porque a menudo se ejecuta en sistemas operativos obsoletos y sin parches. Los cajeros automáticos se componen de *hardware y software* complejos y específicos, lo que significa que pueden ser difíciles de actualizar tanto desde la perspectiva de los sistemas como desde la del coste.

Otro problema es que los cajeros automáticos deben estar disponibles para los clientes las 24 horas del día, los 7 días de la semana, por lo que el tiempo de inactividad debe ser limitado. Esto dificulta encontrar el momento adecuado para realizar pruebas y actualizaciones. De hecho, el equilibrio entre la disponibilidad y las actualizaciones significa que la tentación de retrasar la realización de cambios o actualizaciones sea alta. Como resultado, las mejoras en las redes de cajeros automáticos se quedan atrás y los bancos luchan por obtener una imagen actualizada de su vulnerabilidad general en términos de superficies de ataque potenciales y puntos específicos de vulnerabilidad.

Por tanto, la gestión y el mantenimiento de estas máquinas suelen estar fragmentados. Además, demasiados usuarios pueden acceder legítimamente a los sistemas y al *hardware*, lo que aumenta el riesgo de que se produzca un ataque. Y el problema de lidiar con cualquier ataque es que luego requiere una actualización, algo muy costoso de implementar. Incluso cuando los proveedores han implementado actualizaciones para solucionar esto, los atacantes han encontrado formas de evitarlas.

Para enfrentar de manera eficaz estos problemas, es necesario buscar soluciones de ciberseguridad a medida, capaces de reducir los riesgos de ciberataques asociados a los cajeros.

EXPLOTAR LAS VULNERABILIDADES: UNA TENDENCIA AL ALZA

En primer lugar, deben identificarse los principales ciberataques de los que es víctima la red de cajeros automáticos y luego los bancos podrán encontrar la mejor manera de protegerla.

ATAQUES LÓGICOS

Estos ataques a los cajeros automáticos han ido creciendo sin cesar en la última década, ya que las recompensas son altas y se pueden realizar de forma silenciosa. Los delincuentes pueden llevarlo a cabo e en una red de cajeros automáticos en varios ATMs simultáneamente en lugar de explotar uno solo. Existen diferentes tipos de ataques lógicos, en constante evolución y cada vez más sofisticados.

ATAQUES *MitM (man in the middle)* O INTERMEDIARIO

Esta es otra tendencia que parece haber llegado para quedarse. Se produce cuando un ciberdelincuente intenta secuestrar una operación en un cajero automático. Por ejemplo, si un cliente bancario necesita ejecutar una transacción, esta se dirige a un centro de autorización que verificará si es una transacción válida. Los atacantes intentarán aprovechar esto manipulando los mensajes que solicitan la autorización de la transacción y sSi pueden acceder a ellos, pueden engañar a las víctimas potenciales.

ATAQUES DE CAJA NEGRA

Otro tipo de ataque que aumentará en 2021 es el llamado *black box attack*, un ataque físico que no se basa en *malware* o tecnología, sino en el dispositivo externo físico y de conexión, como el dispensador del cajero automático. Al conectarse al dispensador, el dispositivo externo puede emitir comandos de dispensación, lo que provoca que salga efectivo del cajero automático.

El hecho de que la mayoría de los cajeros automáticos a menudo tenga barreras físicas deficientes contribuye al aumento de los ataques de caja negra: los delincuentes pueden acceder fácilmente al *hardware* físico. Otra razón por la que están en alza se debe al hecho de que la técnica en sí es más barata y sencilla de realizar que otras fraudulentas, como la clonación de tarjetas o el *skimming* de cajeros automáticos. Además, los delincuentes menos cualificados pueden comprar fácilmente el equipo para llevarlos a cabo.

Si bien la mayoría de los ciberdelincuentes ejercen estos ataques en ATMs no bancarios, el reciente aumento de los ataques a los cajeros de las sucursales bancarias ha demostrado que son igualmente vulnerables.

JACKPOTTING

Esta es una técnica similar al ataque de caja negra, mediante el cual los ciberdelincuentes usan *malware* para engañar a un cajero automático para que entregue efectivo. Es muy fácil de llevar a cabo y ha crecido en los últimos años. No hay duda de que continuará en 2021.

Una de las razones por las que seguirá siendo tendencia se debe a que los ciberdelincuentes se están esforzando mucho en desarrollar formas innovadoras de atacar a través de la capa XFS.

El problema nuevamente con el canal de cajeros automáticos es que estos son físicamente accesibles; los atacantes pueden acceder a ellos infiltrándose en la infraestructura bancaria y obtener así acceso al efectivo. También contienen datos confidenciales, como los números de tarjetas de crédito y PIN.

Una vez más, las vulnerabilidades de los obsoletos sistemas de cajeros automáticos han contribuido al aumento global del *jackpotting*. Como se ha mencionado ya anteriormente, muchos cajeros automáticos funcionan con versiones de Windows de hace una década. Esto da a los hackers la oportunidad de infiltrarse en sus capas de *software* y explotar el *hardware* para activar el dispensador de efectivo.

NUEVO OBJETIVO: LOS DISPOSITIVOS DE AUTOSERVICIO

Los cajeros automáticos no son el único objetivo de los delincuentes. De hecho, con la creciente prevalencia del trabajo en remoto y en casa, los empleados bancarios solo tienen acceso remoto a sus sistemas. Esta área también revela debilidades que pueden explotar los ciberdelincuentes. Utilizar soluciones específicas de ciberseguridad en los ordenadores de los empleados será inevitable.

Por ejemplo, los dispositivos de autoservicio asistido, que son propiedad por completo y están asegurados por una institución financiera, que serán la interfaz entre el cliente y la entidad en el banco del futuro, deben estar suficientemente protegidos para ganarse la confianza de los clientes. El aspecto de la seguridad puede convertirse en un diferenciador importante frente a otros canales, como el *online* o el móvil, que el cliente también es responsable de proteger.

En términos de riesgos, el fraude financiero obviamente seguirá siendo uno de los factores clave para un ciberataque, pero una amenaza aún más dañina para la confianza y seguridad de las sucursales bancarias *lean* sería un ataque dirigido a blancos específicos. Esto conduciría a una filtración de datos del cliente, la interrupción de la continuidad del negocio, un daño a la reputación de la institución financiera y la pérdida de la confianza del cliente en el servicio (en comparación con otros canales bancarios).

Al igual que los cajeros automáticos, los dispositivos de autoservicio asistido son físicamente accesibles y dependen de las comunicaciones remotas y de la interconexión con la infraestructura de TI, heredando algunos de sus riesgos y vulnerabilidades. Por lo tanto, es necesario implementar una estrategia de ciberseguridad de Tecnología de Operaciones (OT por sus siglas en inglés) eficaz. Un enfoque de ciberprotección integral y sólido es una necesidad absoluta, pero debe complementarse con la monitorización proactiva del dispositivo, en términos de disponibilidad del servicio y estado de seguridad, y de la capacidad de tener acceso en tiempo real para investigar y remediar cualquier incidente de seguridad potencial.

Las entidades financieras tendrán que analizar más intensamente 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.

CONFIAR EN LA INTELIGENCIA ARTIFICIAL Y EL APRENDIZAJE AUTOMÁTICO PARA LA CIBERSEGURIDAD

La inteligencia artificial (IA) y el aprendizaje automático (ML, Machine Learning, en inglés) están desempeñando un papel cada vez más importante en la ciberseguridad, con herramientas de seguridad que analizan datos de millones de ciberincidentes y los utilizan para identificar amenazas potenciales: una cuenta de un empleado que actúa de manera extraña al hacer clic en enlaces de *phishing*, por ejemplo, o una nueva variante de *malware*. Un beneficio clave del aprendizaje automático en ciberseguridad es que identifica y reacciona ante problemas sospechosos casi de inmediato, evitando que los problemas potenciales interrumpan el negocio.

Al implementar la ciberseguridad basada en inteligencia artificial para automatizar algunas de las funciones de defensa, el objetivo es garantizar que la red sea segura, sin depender de que los humanos tengan que realizar la tarea imposible de monitorizar todo a la vez.

Pero, aunque la ciberseguridad basada en IA tiene muchos beneficios, no es una sustituta completa para el personal de seguridad humano; y como cualquier otro *software* en la red, no puedes simplemente instalarlo y olvidarte de él, es necesario realizar una evaluación periódica. No se puede asumir que la inteligencia artificial y el aprendizaje automático vayan a resolver todos los problemas.

SOLUCIONES PROBADAS PARA LA SEGURIDAD INTEGRAL DE LOS DISPOSITIVOS

La solución Lookwise Device Manager (LDM) de Auriga permite a los equipos de seguridad bancaria monitorizar el estado de seguridad de la red bancaria desde una única interfaz gráfica, evitando la necesidad de gestionar múltiples soluciones independientes.

Este enfoque centralizado también significa que la gestión de los dispositivos y de la infraestructura se puede realizar dentro de un único centro y que se pueden ejecutar acciones de forma remota para establecer rápidamente nuevas defensas, mediante técnicas que incluyen la segmentación de la red y la implementación de nuevos cortafuegos.

Las diversas capas de protección necesarias incluyen protección de la integridad de los archivos, listas blancas de aplicaciones, cifrado completo del disco y protección del *hardware*. Estos actúan de forma singular y conjunta para proporcionar un robusto elemento disuasorio para los posibles atacantes. Y, debido a que se pueden administrar de forma centralizada, permiten que el banco tenga visibilidad sobre dónde podría haber una vulnerabilidad y cómo corregirla para evitar que se convierta en un problema sistémico más amplio.

LDM es una solución de seguridad integrada multiproveedor que proporciona el modelo de protección en capas más avanzado para dispositivos de autoservicio, lo que permite monitorizar el estado del sistema operativo o XFS y los eventos de seguridad relevantes.

La solución también cuenta con un módulo de carga de clave remota (RKL) que está integrado en las otras capas y proporciona diferentes módulos para controlar de forma remota los dispositivos ATM, facilitando así las operaciones, las investigaciones de seguridad y las actividades de mantenimiento.

El gestor trabaja agregando una capa de control adicional para que los equipos de operaciones puedan administrar el proceso de carga remota de claves y ejecutar acciones remotas personalizadas para investigar o reaccionar a la nueva generación de ataques lógicos y físicos basados en *malware*.

Esto proporciona un medio centralizado y eficaz para gestionar la seguridad de los terminales bancarios individuales. El gestor cubre todos los tipos de ataques al bloquear los intentos de infectar los cajeros automáticos con *malware* y evitar así que se ejecute cualquier penetración exitosa de *malware*.

En la práctica, esto significa que una vez que se ha intentado un ataque, el banco puede tomar medidas para detener su propagación por la red de cajeros automáticos cerrando el área afectada, en lugar de toda la red.

Proporcionar las medidas de seguridad adecuadas para proteger cada puesto de trabajo de una organización es una misión esencial. Los puestos de trabajo seguros son la base de las redes seguras, ya que, si un *hacker* puede acceder a uno de ellos, toda la red podría verse comprometida. Cualquier solución de seguridad debe incluir antivirus, prevención de copias de seguridad, cortafuegos, mantenimiento y monitorización remotos. LDM ofrece una solución integral para todos los dispositivos de la sucursal, que simplifica el proceso de seguridad y supervisión. La tecnología utiliza el concepto de listas blancas para permitir el acceso a los recursos del sistema de manera controlada.

En última instancia, no invertir en la tecnología adecuada significa que los bancos corren el riesgo de abrirse a la posibilidad muy real de experimentar violaciones de seguridad, pérdida de datos confidenciales de los clientes y, por supuesto, robo de dinero. El daño a la reputación es simplemente demasiado grande.
Es hora de actuar.

AURIGA
the banking e-volution

Auriga Latin America, S.de R.L.de C.V.
Rio Pánuco 108, Cuauhtémoc, 06500,
Ciudad de México, México
www.aurigaspa.com
mexicocity@aurigaspa.com