CAJEROS AUTOMÁTICOS

EL NUEVO FOCO EN LA CIBERSEGURIDAD DE LOS BANCOS

ARTÍCULO DE OPINIÓN

THE # NEXTGENBANK®

AURIGA
the banking e-volution

www.aurigaspa.com

La banca se ha convertido en uno de los principales objetivos de los ciberataques a nivel mundial por la rapidez con la que se puede obtener dinero mediante el acceso a la información personal de los clientes. Sin embargo, no ha pasado desapercibido para los ciberdelincuentes que existe una vía aún más rápida de obtener su botín: los cajeros automáticos.

Mediante técnicas como el '*jackpotting*', los ciberdelincuentes explotan las vulnerabilidades físicas y de *software* de estos dispositivos para acceder al dinero en efectivo. Gracias a su simplicidad, estos ataques se han popularizado enormemente, con un coste para las entidades bancarias de millones de euros. Por dar algunas cifras, el *malware* de cajeros Ploutus ha causado pérdidas de 450 millones de dólares (398 millones de euros) en todo el mundo desde que apareciera en México en 2013.

El progresivo perfeccionamiento de estas técnicas de explotación de los puntos débiles en los sistemas bancarios ha llevado a las entidades a virar hacia una posición defensiva en la que el primer paso es detectar las vulnerabilidades en su red para poder establecer soluciones de protección de forma integral.

LOS ATMS EN EL PUNTO DE MIRA DE LOS DELINCUENTES

Principalmente existen dos tipos de ataques con los que los delincuentes obtienen efectivo de los cajeros automáticos. Por un lado, la introducción de *malware* (ataque lógico); por otro, los ataques a la caja negra de los cajeros (ataque lógico / físico). El factor determinante para que estos dispositivos sean tan accesibles es que a menudo, la monitorización que se realiza de su estado es deficiente. Además, la cantidad de agentes implicados -instituciones financieras, instaladores, proveedores de servicio y desarrolladores, entre otros- hace que sea complicado establecer una estrategia de ciberseguridad integral.

Otra de las problemáticas que debilitan la seguridad de estos dispositivos es la falta de actualización de sus sistemas. Un proceso difícil y costoso, al estar compuestos por un ecosistema complejo que combina *software* y *hardware*. Por ejemplo, muchos cajeros aún utilizan Windows 7, un sistema que Microsoft ya no soporta. De hecho, Auriga estima que el 40 % de los cajeros automáticos en todo el mundo opera con sistemas operativos aún más obsoletos (como Windows XP-OS), que no son compatibles con Microsoft desde 2014, convirtiéndolos en dispositivos aún más vulnerables a los ataques.

Un *hardware* y *software* desactualizados pueden resultar en la penalización de la entidad por el incumplimiento de las regulaciones PCI (normativa internacional de seguridad), pero la tecnología genérica de protección *endpoint* como la diseñada para dispositivos como ordenadores y portátiles no es suficiente para proteger las redes de los ATMs, sino que requieren de soluciones específicas de OT (Tecnología de las Operaciones).

CÓMO ENCONTRAR LA SOLUCIÓN CORRECTA PARA PROTEGER DISPOSITIVOS Y SISTEMAS

Para evitar los ataques con *malware* y otras técnicas utilizadas por los cibercriminales, los bancos necesitan invertir en una solución integral de ciberseguridad específica para cajeros automáticos u otros dispositivos de autoservicio que permita un control remoto y monitorización completa y en tiempo real de la red de cajeros. Lookwise Device Manager (LDM), la solución de ciberseguridad de Auriga para ATMs, ofrece una elevada protección integrada en una única plataforma y ejecutada en varias capas:

Las diferentes capas son:

- **Cifrado de disco completo** de todos los discos duros y volúmenes: evita que los ciberdelincuentes realicen ingeniería inversa para introducir *malware* en el disco duro y luego reemplazarlo en otra sucursal del banco.
- **Protección de la integridad del sistema de ficheros** para bloquear cualquier intento de modificar un archivo crítico, a no ser que el proceso de actualizaciones de *software* esté predefinido.
- **Lista blanca de aplicaciones:** previene la ejecución de *malware* o *software* no autorizado definiendo una lista blanca de procesos que pueden ejecutarse en el cajero automático.
- **Protección de *hardware*:** evita la conexión de *hardware* fraudulento, bloqueando dispositivos que no estén incluidos en la **lista blanca**.

Aplicar este tipo de tecnologías, además de un correcto mantenimiento de las redes de cajeros, permite a los bancos defenderse frente a los crecientes ataques. Sin embargo, las técnicas de los delincuentes están en constante evolución y en búsqueda de ataques más sofisticados con los que identificar nuevas vulnerabilidades, por lo que es importante que los bancos sean proactivos en la implementación de soluciones, la búsqueda de nuevos métodos de defensa y mediante la involucración de consultorías de seguridad especializadas para comprobar los planes y procesos de seguridad.

De cualquier modo, es importante recordar que cabe la posibilidad de que una variante de *malware* logre acceder al sistema, y ante esta situación es recomendable que los bancos hayan elaborado un plan de actuación que permita una rápida recuperación del negocio.

En este sentido, es posible emplear la inteligencia de amenazas cibernéticas (CTI por sus siglas en inglés) para una detección temprana de las potenciales amenazas, ayudando a las entidades bancarias a comprender dónde se encuentran sus puntos débiles y como se pueden explotar, además del impacto potencial de una incursión en sus sistemas. Por último, será clave la colaboración con los desarrolladores de *software* y organizaciones financieras para asegurar una integración total de las soluciones de seguridad mediante la cooperación de todos los agentes implicados.

ARTÍCULO DE OPINIÓN

THE # NEXTGENBANK®

AURIGA
the banking e-volution

Auriga Iberia, S.L.
Calle Villalar 7, Bajo Izquierda,
28001 Madrid - Spain
www.aurigaspa.com
madrid@aurigaspa.com