NOTA DE PRENSA

10 claves de ciberseguridad para proteger los cajeros automáticos y las operaciones bancarias

Los cajeros se consideran infraestructuras críticas y su vulnerabilidad puede afectar a todo el sistema de seguridad

Madrid, 28 de julio de 2020 – Con la reciente crisis sanitaria y el consecuente confinamiento, los niveles de ciberdelincuencia han aumentado de forma notable, especialmente en el caso de los ataques a sistemas bancarios. No es un fenómeno nuevo: en los últimos seis años, los ataques a cajeros automáticos con el virus Ploutus han supuesto el robo de 500 millones de dólares. Las entidades necesitan soluciones de seguridad para proteger la integridad de los sistemas, prestando atención a los puntos más vulnerables, los cajeros automáticos, considerados infraestructuras críticas. Para garantizar su protección y blindar los sistemas, **Auriga, especialista en aplicaciones de *software* para cajeros automáticos y sistemas de pago destaca 10 puntos a tener en cuenta:**

1. **Inversión en tecnología y actualización de sistemas:** un porcentaje elevado del presupuesto de las entidades bancarias se destina a la adquisición de tecnología. Sin embargo, en el caso de los cajeros encontramos sistemas operativos antiguos y con falta de actualizaciones, lo que puede generar una brecha en la seguridad de todo el sistema.

2. **Cifrado de discos duros y volúmenes:** este aspecto es imprescindible para cualquier banco que quiera proteger su red de cajeros automáticos. Sin ello, los delincuentes pueden realizar ingeniería inversa en el *hardware* para introducir *malware* en el disco duro y luego reemplazarlo en otra sucursal del banco.

3. **Mantener la integridad de los archivos:** todos los archivos binarios de un cajero automático son críticos, por lo que una solución de ciberseguridad efectiva debe centrarse en asegurar que no son accesibles ni editables y que permanecen incorruptos.

4. **Proteger el *hardware*:** uno de los puntos críticos de los ataques a cajeros automáticos es la introducción de *hardware* con el que poder tomar el control del dispositivo. Para proteger el sistema, es necesario contar con un

método de cortafuegos que bloquee cualquier intento de conexión que no provenga del propio *hardware* del cajero.

5. **Soluciones enfocadas en la tecnología de operaciones (TO):** generalmente, el *software* instalado en los cajeros automáticos está enfocado a dispositivos *endpoint* como ordenadores, pero un cajero hace un uso mucho más limitado del *software*. Al restringir el número de aplicaciones que pueden ejecutarse, se logra reducir la superficie de ataque y se evita que los atacantes puedan utilizar *software* legítimo para perpetrar ciberataques.

6. **Limitar las comunicaciones de red:** una solución efectiva para proteger la integridad de un cajero automático debe asegurar una comunicación limitada, impidiendo que un programa externo se conecte con el servidor del banco.

7. **Monitorizar el sistema en tiempo real:** el control del sistema en tiempo real ofrece una mayor capacidad de reacción y permite adelantarse a posibles fallos o riesgos mayores.

8. **Lograr una gestión remota:** la posibilidad de gestionar todo el sistema de forma remota aumenta la capacidad de reacción ante un ataque, ya que permite hacer ajustes desde cualquier lugar, sin tener que personarse en la entidad.

9. **Formar al personal de la entidad en ciberseguridad:** una correcta formación del equipo es siempre una ventaja frente a los ciberataques. La formación específica sobre los sistemas de seguridad implantados evita errores humanos que propicien un ataque o una brecha en el sistema.

10. **Adelantarse a los ciberdelincuentes:** por último, uno de los procesos determinantes en la protección de la infraestructura tecnológica de los bancos es investigar constantemente para adelantarse a las maniobras de los delincuentes, que de forma continua desarrollan nuevos métodos para acceder a los sistemas informáticos.

La solución Lookwise Device Manager de Auriga establece una protección total de los sistemas de cajeros automáticos mediante capas, asegurando la integridad de los archivos, el cifrado de los discos y la limitación del software ejecutable, mientras ofrece una gestión remota del sistema.

"A día de hoy, los ataques se crean en una parte del mundo y se globalizan, pudiendo utilizarse en todo el planeta. Además, son tan sofisticados, que el banco puede tardar

semanas en notar las pérdidas si no actúa rápido", apunta Élida Policastro, vicepresidenta regional de la división de Ciberseguridad en Auriga. *"LDM permite a las instituciones financieras gestionar la seguridad de los dispositivos críticos mediante la protección, la vigilancia y el control de los activos".*

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