NOTA DE PRENSA

Octubre: el mes europeo de la ciberseguridad

Auriga da a conocer los ciberataques más frecuentes, cómo debe actuar una entidad financiera ante ellos y cómo pueden evitarlos los ciudadanos / trabajadores

Madrid, 19 de octubre de 2020– Desde el comienzo de la pandemia, organizaciones como la INTERPOL han alertado sobre el alarmante número de ciberataques producidos durante estos meses. Los ciberdelincuentes se han aprovechado del miedo y la incertidumbre colectivas y de la rapidez con la que los trabajadores han comenzado a teletrabajar -con la escasa seguridad para la información privada y profesional que eso ha supuesto-, para centrar sus ataques en organizaciones gubernamentales y sanitarias, así como en entidades bancarias, uno de los sectores más amenazados.

Auriga, compañía **especialista en aplicaciones de *software* para cajeros automáticos y sistemas de pago,** quiere celebrar el mes europeo de la ciberseguridad haciendo un repaso por algunos de los aspectos que esta engloba.

Los ataques más frecuentes

Los ciberdelincuentes se han dado cuenta de que las redes de cajeros automáticos suelen ser uno de los eslabones más débiles de la infraestructura de seguridad de un banco. Una de las principales razones es que en ellos hay mucho *hardware* y *software* heredados porque es muy caro y difícil de actualizar. Los cajeros automáticos están sujetos a ataques tanto físicos como lógicos por muchos motivos. Dos de ellos son que el efectivo físico actúa como un incentivo y que contienen información privada, como códigos PIN y números de tarjetas de débito, que puede robarse y venderse.

Lamentablemente, esto significa que es probable que estos sistemas sean inseguros. Auriga estima que alrededor del 40 % de los cajeros automáticos de todo el mundo utilizan sistemas operativos antiguos, lo que hace que sean aún más vulnerables a las violaciones. Además, uno de los principales vectores de ataque a los cajeros automáticos es la capa XFS, el *middleware* estándar diseñado para permitir que el *software* de varios proveedores se ejecute en los cajeros automáticos de los fabricantes y en otros equipos. Los ciberdelincuentes despliegan *malware* en dispositivos de *hardware*, como los cajeros automáticos, para dar órdenes de sacar y dispensar dinero, el lector de tarjetas para robar los números y el *pinpad* para aprender la contraseña de identificación.

¿Se pueden evitar estos ciberataques?

Cuando se trata de cajeros automáticos, la tecnología genérica de protección de puntos finales, como las soluciones *antimalware*, no es suficiente, ya que dichas tecnologías están diseñadas para proteger los PC y los portátiles. Los cajeros automáticos son dispositivos de infraestructura crítica -no pueden desconectarse realmente por una cantidad de tiempo concreta para reiniciarlos como un dispositivo móvil-. Las redes y los sistemas de cajeros automáticos deben estar disponibles 24 horas al día, 7 días a la semana, por lo que requieren una mayor protección y un enfoque diferente. La mejor opción es una solución de seguridad centralizada, que proteja, supervise y controle las redes de cajeros automáticos y, de este modo, gestione toda la red de activos bancarios desde un mismo lugar y tome las medidas adecuadas, como impedir que el *malware* se propague por la red desde los cajeros automáticos infectados.

La principal recomendación de la compañía para impedir que las entidades financieras sufran brechas de seguridad es que inviertan en tecnología especializada y en la actualización de sus sistemas, para evitar cajeros con sistemas operativos antiguos, obsoletos. En segundo lugar, es imprescindible cifrar los discos duros y volúmenes, así como mantener la integridad de los archivos, para que no se pueda acceder a ellos, ni editarlos y, por tanto, permanezcan incorruptos.

Igual de importante es la protección del *hardware*, para que no se pueda tener control sobre el dispositivo, ya que previene cualquier conexión fraudulenta, bloqueando los dispositivos que no estaban previamente configurados como válidos en la lista blanca. Otra sugerencia es monitorizar el sistema en tiempo real y en remoto, para contar con una mayor capacidad de reacción. Y no puede faltar la formación al personal que trabaje en la empresa.

La solución de Auriga, Lookwise Device Manager (LDM), es Tecnología Operacional centralizada y modular. No solo proporciona una alta protección de ciberseguridad, sino que también puede ahorrar tiempo y dinero a las organizaciones bancarias, ya que la gestión de los cajeros automáticos y de la infraestructura está centralizada en un único punto y todas las capas de protección se gestionan desde una única consola. Se pueden ejecutar acciones a distancia para establecer rápidamente nuevas defensas. Esto permitirá, por ejemplo, poder analizar una nueva muestra de *malware* que haya sido bloqueada por LDM, analizar su funcionamiento y prevenir su futura ejecución en otros ATMs.

Cómo debe actuar una entidad financiera

Se comprenden perfectamente las razones por las que una empresa evite dar a conocer que ha sufrido un ataque, pero para impedir que una compañía se vea ante esta tesitura, es fundamental que se potencie la cooperación policial internacional,

el intercambio de información entre organizaciones especializadas en ciberseguridad y entidades bancarias y la colaboración global.

Élida Policastro, vicepresidenta regional de la División de Ciberseguridad de Auriga, afirma que *"el confinamiento y el teletrabajo nos ha hecho más dependientes de la conectividad que nunca, lo que ha facilitado el trabajo de los ciberdelincuentes, sobre todo porque el escenario actual no cuenta con los recursos suficientes y la seguridad necesarias para hacerlo. Cada día se crean nuevos ataques, cada vez más intensos, globalizados y a un ritmo vertiginoso, por lo que hay que ser proactivos y estar lo más preparados posible".*

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