Ciberseguridad: una prioridad para la banca en 2021

Con la llegada de la pandemia, uno de los objetivos principales de la ciberdelincuencia son las entidades bancarias

Madrid, 2 de diciembre de 2020-. El creciente uso de los canales digitales y la disminución de posibles víctimas en las calles debido a las medidas de confinamiento ha empujado a los ciberdelincuentes a explotar formas más sutiles de delinquir mostrando un **especial interés en las entidades financieras** y utilizando técnicas cada vez más sofisticadas. A medida que los ataques se vuelven más complejos, los sistemas de defensa de las entidades también deben evolucionar.

Dependiendo de la potencia del ataque, las entidades pueden quedar paralizadas durante semanas, intentando **recuperar el control** de sus sistemas. Por eso es de vital importancia que protejan su infraestructura, empezando por puntos críticos como los cajeros automáticos.

Algunos datos sobre el cibercrimen en los últimos meses:

- Según datos recogidos por Hackmageddon, de los ciberataques realizados en septiembre de 2020, un 85,6 % respondían a una **motivación criminal** -un 1,3 % más que en el mismo mes del año pasado- frente a un 1,5 % con una motivación *hacktivista*, un 1,5 % tras la ciberguerra y un 11,4 % de ciberespionaje.

- Los ataques al sector financiero han supuesto un 6,5 % del total de ataques, prácticamente el doble que el año pasado, además de un 1,5 % enfocados en las empresas *fintech*.

- La técnica más utilizada por los ciberdelincuentes en sus ataques a entidades financieras es el *ransomware*, que consiste en un **secuestro de información** por medio de su cifrado para posteriormente pedir una cantidad económica a cambio de liberarla.

- Según el noveno estudio anual sobre costes del cibercrimen elaborado por Accenture, los bancos, financieras y aseguradoras invierten anualmente 18,5 millones de dólares para combatir la ciberdelincuencia.

Ataques lógicos: ¿qué medidas pueden tomar los bancos para prevenirlos?

Los ataques a entidades bancarias causan pérdidas de billones de dólares en todo el mundo y suponen un **riesgo directo** para los usuarios finales si además se accede a las bases de datos o se infectan los servidores para redirigir a los clientes a webs similares, realizando estafas de tipo *pharming*.

Además, entre los puntos de contacto de los bancos, los cajeros automáticos, en concreto, representan el eslabón más débil. En los últimos años se han convertido en un blanco fácil para los ataques de *jackpotting*, que permiten hackear el dispositivo, convirtiéndolo en una 'máquina tragamonedas' a la merced de los cibercriminales. Para **mantener seguras las infraestructuras de cajeros automáticos**, Auriga, especialista en banca omnicanal y seguridad, sugiere cinco medidas preventivas principales:

- El primer paso es contar con un sistema robusto, monitorizable en tiempo real y de forma remota que permita conocer el estado de las comunicaciones en todo momento.
- El acceso a discos duros debe estar cifrado para evitar incursiones y robos de información que puedan afectar seriamente a la infraestructura del banco.
- Los sistemas deben permanecer siempre actualizados y centrarse en tecnologías operacionales, acotando las funcionalidades de dispositivos como los cajeros automáticos.
- Mantener la integridad de los archivos asegurando que no son accesibles ni editables.
- Limitar las comunicaciones de red evitando que programas externos se conecten al servidor del banco.

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, protegen a los dispositivos críticos de los ciberataques y crean una ventaja competitiva a largo plazo. Auriga es una compañía global con una presencia activa en Europa y operaciones en expansión en Reino Unido, Latinoamérica y en Asia-Pacífico

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