CIBERATAQUES BANCARIOS

LA SILENCIOSA CONSECUENCIA DEL COVID-19

ARTÍCULO DE OPINIÓN

AURIGA
the banking e-volution

THE # NEXTGENBANK®

www.aurigaspa.com

Entre los cambios que trajo el Covid-19 a nuestras vidas, uno de los más relevantes es el crecimiento en la adopción del teletrabajo. Si bien al inicio nos parecía una idea fantástica el poder laborar desde la comodidad del hogar, lo cierto es que esto hace algún tiempo que ya cobró factura.

No solo por lo agobiante que pueden resultar las jornadas laborales, sino porque el home office ha abierto una peligrosa puerta de entrada para los fraudes cibernéticos, sobre todo en el sector financiero, donde las entidades han perdido millones de dólares por acción de los ciberdelincuentes.

Por ejemplo, con el aislamiento social las transacciones se volcaron al entorno digital, lo cual ha elevado las alertas ante posibles fraudes. Es justamente en este contexto el cibercrimen ha aumentado aumentando su actividad a través de ataques como el phishing, el mismo que fue el de mayor incidencia, según el estudio de ciberseguridad Estado del Riesgo Cibernético en Latinoamérica en Tiempos del COVID-19, elaborado por Microsoft y Marsh.

Es preocupante que en la actualidad las empresas estén más expuestas al uso de dispositivos personales debido al trabajo remoto, pero lo es más el hecho de que - según la citada investigación - solo el 24% de las compañías haya incrementado su partida de ciberseguridad y que incluso 10%, lo haya reducido.

LOS BANCOS, PRINCIPALES VÍCTIMAS

El riesgo está en todas partes y el sector bancario en Latinoamérica no es la excepción. Las instituciones financieras tienen hasta 300 veces más probabilidades de sufrir un ciberataque que otras empresas, por lo que es imperativo que refuercen sus medidas de ciberseguridad. Esto implica contraatacar tanto en los terminales ATMs, ya que son altamente vulnerables, como en los canales digitales, en los que el fraude ha ido en franco ascenso.

Por ejemplo, en Colombia, la Asociación Bancaria y de Entidades Financieras de Colombia (Asobancaria) dio cuenta de que, en el 2020, alrededor del 41% del fraude en el sistema financiero colombiano se concentró en canales digitales, siendo la banca móvil el punto de concentración de la mayoría de estas reclamaciones (49,83%) y la ingeniería social por teléfono la principal modalidad de ataque (78,05%).

En Chile, por otro lado, antes de la pandemia, alrededor del 20% de los ciberataques utilizaban malware o métodos nunca vistos; sin embargo, esto aumentó al 35%, según la consultora Deloitte. Asimismo, se ha identificado un incremento de 600% del phishing asociado al Covid durante 2020.

En tanto, el Reporte de estabilidad financiera del Banco de México, realizado el primer semestre de este año, señala que ocho de los 10 incidentes cibernéticos que han sido reportados por instituciones financieras en el primer semestre del 2021 fueron específicamente contra cajeros automáticos

Entre los principales ataques, además del Phishing y Ransomware, se encuentran el spear y voice phishing, que consisten en obtener datos a través de enlaces de sitios falsificados y en hacer llamadas usurpando a ejecutivos bancarios para sustraer información, respectivamente.

Estas entidades son plenamente conscientes de las amenazas a las que están expuestas, por lo que en muchos casos no han dudado en implementar tecnología para hacer frente a estos riesgos. No solo han incrementado sus presupuestos, sino que han hecho despliegue de campañas educativas dirigidas a sus usuarios finales con el objetivo de contrarrestar la ingeniería social.

PREVENCIÓN Y TECNOLOGÍA DE AVANZADA

Para evitar ataques basados en la red a los cajeros automáticos las instituciones financieras deben implementar tecnología de última generación para poder hacer frente a las ciberamenazas.

Una buena opción es la segmentación de la red corporativa, es decir, dividirla en diferentes áreas que están solo parcialmente en red o no lo están en absoluto. De esta manera, el entorno de los ATMs estará separado del resto de la red de TI corporativa evitando tráfico extraño.

En este aspecto la inteligencia artificial y el aprendizaje automático cobran cada vez más protagonismo en la detección temprana de ataques. Varias herramientas de seguridad analizan datos de millones de incidentes cibernéticos y los utilizan para determinar amenazas potenciales, llegando a diferenciar una transacción real de una fraudulenta.

Las listas blancas constituyen otra tecnología para permitir el acceso controlado a los recursos del sistema. De esta manera, si un usuario proporciona información personal durante una videollamada o una consulta remota, los puertos USB podrían bloquearse para impedir su almacenamiento en un dispositivo externo.

En esta lucha es clave la cooperación entre los desarrolladores de software y las organizaciones financieras. De este modo, se asegurará la integración adecuada entre proveedores de hardware, software y soluciones de seguridad para cajeros automáticos y las compañías que los gestionan.

La investigación permanente es otro de los pilares para hacer frente a los ciberdelincuentes, debido a que siempre están desarrollando nuevas maneras para vulnerar los sistemas informáticos de los cajeros automáticos y de las plataformas que ofrecen servicios bancarios a los clientes.

En conclusión, garantizar la protección de los entornos críticos solo se puede lograr con soluciones integrales que permitan proteger, monitorear y controlar de manera centralizada las redes de cajeros automáticos.

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