RETROSPECTIVA Y PROYECCIÓN DE CIBERSEGURIDAD PARA EL SECTOR FINANCIERO EN LATAM

Recibido: 06 de octubre de 2023
Aceptado: 19 de junio de 2024

Autor (es)

Brayan Alberto Granados Sanchez
Ingeniero Ciberseguridad

En el ámbito de la ciberseguridad, las tendencias de amenazas emergentes aplicables para el sector financiero en LATAM con el avance de las tecnologías van a tener mayor relevancia en las operaciones bancarias, actualmente los niveles de criminalidad continúan en auge a nivel mundial haciendo uso de distintos escenarios, pero sin duda el que ha tomado mayor relevancia es el cibercrimen que también es usado en la guerra que afrontan las grandes potencias mundiales en algunos casos con influencia directa de los estados de gobierno motivo por el cual se considera una amenaza de alto riesgo para la estabilidad de las economías y el bienestar de la humanidad.

En la era actual que también es conocida como la revolución tecnológica se han posicionado tres problemas que generan preocupación en las personas, las empresas y la sociedad en general como lo son el cibercrimen, la desinformación y la pérdida de la privacidad en el entorno digital. En el campo empresarial, y más exactamente el sector financiero se encuentra dentro del grupo de sectores a nivel global que representan mayor apetito por los ciberdelincuentes para perpetrar ataques cibernéticos y ha dado la oportunidad para crear organizaciones debidamente estructuradas para llevar a cabo sofisticadas acciones que incluso han colapsado la estabilidad tecnológica para la prestación de servicios financieros.

La alta rentabilidad que representa el diseño y ejecución de ciberataques que se traducen en modalidades de crimen desde el anonimato incentivan a nuevas modalidades ilícitas que fortalecen las capacidades de inestabilización de infraestructuras tecnológicas, el colapso empresarial, el miedo en las personas por hacer uso de las tecnologías y la incertidumbre de lo que pueda suceder a futuro. Este panorama ha hecho reaccionar a los diferentes gobiernos y centrar sus esfuerzos en trabajar para rastrear y desmantelar grupos cibercriminales haciendo sinergias con organismos internacionales de seguridad y ciberdefensa para contrarrestar las acciones ilícitas de estos grupos. Sin lugar a dudas la pandemia por Covid-19 que el mundo vivió a partir del año 2020 fue una importante oportunidad para los ciberdelincuentes ya que las personas sin discriminar su rango de edad, tuvieron que adaptarse al uso de las tecnologías multiplicando la interacción con los diversos recursos digitales y exponencialmente estar más expuestas a riesgos de seguridad de la información. Latinoamérica no es ajena a esta problemática ya que desde el 2020 se ha evidenciado el elevado aumento de ciberataques y obligando a las empresas a invertir altos recursos financieros para adquirir herramientas tecnológicas, recursos humanos y servicios de protección digital para salvaguardar su información, aplicar medidas de defensa y ofensiva a los ciberdelincuentes significando grandes esfuerzos para evitar pérdidas económicas, reputacionales o sanciones legales que pudieran poner en riesgo su estabilidad en el mercado *(Informe controlrisks)*.

El sector financiero en LATAM ha optado por estrechar los lazos colaborativos para hacer frente al cibercrimen y siendo consciente de la problemática ha tenido que conformar grupos especializados que interactúan entre los distintos países de la región para atender los desafíos de la ciberseguridad en su sector. Se ha hecho necesaria la evolución en los modelos de respuesta ante los ataques cibernéticos determinando cinco importantes tendencias como lo son que exista mayor colaboración entre equipos de respuesta a incidentes de ciberseguridad, rastreo de ataques centrados en la obtención fraudulenta de datos, identificación del comportamiento de los ciberdelincuentes, el aumento en la disponibilidad para detectar oportunamente comportamientos anómalos en los sistemas informáticos y la ciberresiliencia tecnológica ante ciberataques. *(Informe CiberLATAM).*

¿Cuáles son las ciberamenazas más relevantes para el sector?

Desarrollando un análisis del estado actual de la ciberseguridad en el sector financiero donde refleja un aumento de las amenazas cibernéticas, las actividades hacktivistas, relacionando actores de amenazas más polarizados, innovadores, exactos y de mayor impacto. Todo esto hace que la importancia del contexto geopolítico actual representa el traspaso de los escenarios de guerra en los territorios físicos al espacio digital donde lo que se busca es disminuir al adversario y los daños causados están orientados a generar disrupción de servicios tecnológicos, fuga de información sensible y sabotaje a sistemas informáticos. De acuerdo con las particularidades de los diversos informes generados por organismos de investigación de criminalidad cibernética *(Informe ciberseguridad LATAM Infobae)* enfocados al análisis de las amenazas digitales que han sido tendencia en el último año aplicable al sector financiero en LATAM, se encuentran principalmente:

Malware

La aparición de malware basado en código abierto que permite que cada vez se generen más patrones de malware con nuevas y más sofisticadas capacidades de invasión y destrucción donde se destacan RATs, malware dirigido a canales transaccionales financieros y troyanos bancarios. Uno de los más relevantes y que ha hecho ahondar esfuerzos en las entidades financieras se describe como el malware Zanubis del que se han observado campañas en LATAM. *(Informe Zanubis Kaspersky)* Por lo cual es probable que para el año 2024 se continúen detectando nuevas cepas de malware e indudablemente sigan representando un alto riesgo digital para la región.

Ransomware

Esta modalidad sigue siendo una de las modalidades que ha impactado ampliamente no solo el sector sino otros sectores empresariales la cual ha generado escenarios disruptivos en diferentes compañía a nivel mundial dejando al descubierto las brechas de seguridad de empresas sólidas en sus mercados, se destaca como una de las que genera mayor impacto cuando se materializa por su amplio poder de propagación y afectación de servicios tecnológicos donde literalmente llega a detener las operaciones de las empresas que se ven afectadas, su tendencia ascendente en el número de ataques en el primer periodo de 2023 supero el total de lo registrado en el año anterior *(Informe ciberseguridad Infosecurity)*.

Un estado de crisis por causa de ransomware implica bastantes costos no contemplados para una compañía que van relacionados con la investigación, asignación de recursos humanos, análisis forenses, atención de aspectos legales, compensaciones por perjuicios, reclamaciones de primas de seguros entre otros, afectando directamente la competitividad y la confianza empresarial de sus clientes. *(Informe ciberataques Sentinel One)*.

Servicios Cloud Inseguros

Dado el auge de los modelos de servicio cloud, este entorno causa una especial motivación para los ciberatacantes por sus limitantes para tener gestión directa de seguridad sobre estos entornos además de las inadecuadas configuraciones de ciberseguridad que en muchas ocasiones quedan a cargo del proveedor de servicio cloud. *(Estado de seguridad cloud 2023 IT Digital Security)*.

Ciberespionaje

Las entidades financieras por ser una parte fundamental del movimiento y evolución de la economía global siempre son una fuente de motivación por parte de los ciberdelincuentes ya que no solo materializar ataques con fines económicos les genera rentabilidad, sino el interés por tener posesión de información financiera privilegiada y el acceso a información estratégica del sector (información bursátil y fiscal), tecnologías en desarrollo al servicio de la innovación en los servicios financieros y otra información de interés.

El impacto de este tipo de ataque recae en la afectación de la confidencialidad de información sensible y pérdida de ventaja estratégica en proyectos e inversiones puede repercutir en afrontar dificultades por sanciones legales. Esta táctica seguramente podrá continuar de manera incremental con fines de ciberespionaje como consecuencia de la situación geopolítica del mundo actual donde se busca tener ventaja a costa de debilitar al adversario mediante el poder de tener acceso a la información.

Finalmente, las amenazas cibernéticas y la explotación de vulnerabilidades continuarán acentuándose a nivel global y LATAM no será ajena a esto, por eso será importante mantener la colaboración entre equipos de respuesta articulados sin el miedo a interactuar con el mundo exterior ya que de la misma manera como los ciberdelincuentes han encontrado la manera de aliarse entre sí haciendo sinergias para ser más destructivos con sus fines ilícitos, las entidades financieras respaldadas por sus respectivos gobiernos deberán fortalecer sus vínculos, estrategias y políticas de seguridad digital estableciendo mecanismos de comunicación bidireccional para estar en las capacidades de atender oportunamente las amenazas que evolucionan cada día. También será indispensable estar en contacto con otros sectores para afianzar los planes de aseguramiento de infraestructuras críticas, el endurecimiento de las políticas de seguridad digital como parte de las iniciativas gubernamentales para la defensa y soberanía nacional haciendo hincapié en desarrollar programas de inteligencia en profundidad sobre amenazas emergentes guiando a las instituciones para la realización de acciones que estén enfocadas en la reducción de los riesgos y permitan adelantarse al comportamiento de los ciberatacantes lo que supondrá un apoyo al direccionamiento estratégico de las organizaciones para la optimización de esfuerzos en la ciberresiliencia empresarial.