Perspectivas de amenazas cibernéticas en México

Diciembre 2021

El panorama de amenazas cibernéticas en **México** continúa evolucionando, con un número creciente de actores y motivaciones que apuntan a ciertas empresas y organizaciones en el país. Según el Informe sobre Delitos en Internet de 2020 publicado por el FBI, **México** fue el noveno país más atacado a nivel mundial, ocupando el primer lugar en **América Latina** por delante de **Brasil**, con un aumento constante en el número de incidentes reportados en los últimos años.[1]

La gran economía y la rápida digitalización de México, junto con las deficiencias persistentes en la capacidad y la cultura de la seguridad cibernética, continúan motivando a una variedad de actores de amenazas cibernéticas a atacar el país. Las importantes interrupciones provocadas por COVID-19 también han llevado a un aumento del delito cibernético, y el cambio en las prácticas laborales significa que las organizaciones enfrentarán desafíos para adaptarse a la "nueva normalidad", sobre todo en lo que respecta a la seguridad cibernética.

Amenaza ciberdelincuente cada vez más compleja

Las amenazas cibernéticas en México son impulsadas en gran medida por las ganancias financieras, y los ciberdelincuentes llevan a cabo consistentemente los ataques cibernéticos más estratégicamente significativos en el país desde 2017. El fraude cibernético, en particular las tarjetas, el robo de identidad y los troyanos bancarios, representan una amenaza significativa para las personas y las empresas. A medida que el país se ha vuelto más digitalizado, los grupos de crimen organizado tradicionales (GCO) se han aventurado cada vez más en la delincuencia cibernética como una fuente adicional de ingresos y para blanquear ganancias ilícitas. Los grupos regionales de ciberdelincuentes, incluidos los grupos bien establecidos con sede en Brasil, han ampliado cada vez más su alcance en América Latina.

Además, México es un objetivo atractivo para los actores ciberdelincuentes transnacionales. Los grupos de ciberdelincuentes organizados se han dirigido cada vez más a América Latina durante la última década, ya que la madurez de la seguridad cibernética de la región se mantiene por debajo de la de los objetivos tradicionales de dicha actividad, incluidas las economías avanzadas de América del Norte y Europa. Como resultado, las empresas mexicanas, en particular del sector financiero, son atacadas regularmente en campañas motivadas financieramente que utilizan tipos de malware notorio que generalmente se usan para robar las credenciales de los clientes e información personal o facilitar que sean más comprometidas. Las empresas en México también han estado entre los objetivos de campañas globales de fraude por parte de grupos internacionales de ciberdelincuentes, incluidos los que tienen su sede en Rusia y Nigeria.

Imagen 1 ▸ Objetivo de los ataques ciberdelincuentes en México (porcentaje de ataques significativos, enero de 2017-octubre de 2021)

Fraude financiero	52%
Violación o robo de datos	16%
Extorsión	20%
Espionaje comercial	3%
Destrucción de datos	3%
Denegación distribuida de un servicio (DDoS)	3%
Robo de poder de procesamiento	3%

En línea con las tendencias globales más amplias, la prevalencia y el impacto del delito cibernético extorsivo ha aumentado en México en los últimos años, lo que no es menos evidente por los ataques a la petrolera nacional Pemex en noviembre de 2019 y a la Secretaría de Economía poco después en febrero de 2020, aprovechando la misma cepa de ransomware.[2] Recientemente, hemos registrado ataques adicionales de ransomware de alto impacto dirigidos a organizaciones privadas en el país, incluidos el sector financiero y de manufactura, lo que sugiere que las grandes organizaciones del país son cada vez más objetivos atractivos para los operadores de ransomware más capaces a nivel mundial.

El espionaje y las campañas con motivaciones financieras generan una amenaza Estado-Nación

Al igual que con los grupos de ciberdelincuentes, los actores de amenazas extranjeros vinculados a estados se han dirigido principalmente al país para obtener ganancias financieras. En particular, los actores de amenazas vinculados a Corea

[1] https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

[2] https://www.globalsign.com/en/blog/closer-look-latest-cyber-attack-mexican-government

del Norte se han dirigido al sector financiero en América Latina con fraudes a gran escala, incluidos los ataques de 2018 al sistema interbancario local que llevaron a una perdida estimada de 15–20 millones de dólares (USD) en transferencias fraudulentas de bancos en México.[3] Las presiones financieras persistentes debido a las sanciones y la mala situación económica significan que es probable que las campañas de Corea del Norte en América Latina sigan centradas en el fraude financiero durante el próximo año.

Más allá de las campañas motivadas financieramente, las empresas mexicanas son cada vez más un objetivo de los servicios de inteligencia extranjeros como parte de campañas de espionaje globales más amplias que tienen el fin de recopilar inteligencia estratégica sobre políticas clave y desarrollos geopolíticos, así como inteligencia comercial, como datos confidenciales de las empresas y propiedad intelectual. En una campaña descubierta recientemente, se informó que las organizaciones mexicanas se encontraban entre los objetivos de una operación cibernética centrada en sectores estratégicos, en particular telecomunicaciones, junto con TI, medios y finanzas.[4]

Mientras tanto, informes adicionales en julio sobre el uso frecuente de spyware disponible comercialmente por parte de organizaciones gubernamentales mexicanas destacan la capacidad de los actores nacionales para atacar individuos y organizaciones en el país con fines de recopilación de información. Estos diferentes actores y objetivos probablemente continuarán impulsando una creciente complejidad en el entorno de amenazas externas que enfrentan las empresas en México en los próximos años.

Imagen 2 ▸ Objetivo de ataques a estados-nación en México (proporción de ataques significativos, enero de 2017-octubre de 2021)

Espionaje político	38%
Espionaje comercial	19%
Fraude financiero	19%
Infraestructura de recopilación de datos	6%
Destrucción de datos	6%
Desinformación	6%
Lavado de dinero	6%

El sector privado atrapado en el fuego cruzado

La creciente diversidad de las amenazas que enfrenta México es evidente en los patrones de focalización de los actores de amenazas cibernéticas. Como era de esperar, el sector financiero sigue siendo el sector más atacado del país. Las amenazas al sector provienen tanto de ataques dirigidos a clientes como persona física y a clientes como persona moral, por ejemplo, con el objetivo de robar información de tarjetas o cuentas bancarias, así como de ataques más sofisticados dirigidos directamente a las redes y los datos de las instituciones financieras. Como ejemplo, el banco mexicano CIBanco confirmó en agosto de 2020 que había estado sujeto a una intrusión fallida en la red, luego de que los operadores de ransomware afirmaron haber robado y publicado datos corporativos confidenciales en la dark web. Sin embargo, CIBanco afirmó que no se robaron datos.[5] Por lo tanto, es probable que el sector financiero siga siendo un objetivo atractivo para las campañas vinculadas al estado contra el fraude financiero y el blanqueo de capitales.

Si bien las entidades gubernamentales y las empresas de propiedad estatal también se encuentran entre las más afectadas en el país, las empresas del sector privado en industrias clave como son TI y telecom-unicaciones, energía, petróleo y gas, y manufactura son cada vez objetivos más atractivos para los grupos de amenazas cibernéticas por una variedad de motivos. Es probable que los proveedores de servicios de TI, y sus clientes, se enfrenten a una amenaza persistente en donde puedan estar comprometidas sus cadenas de suministro en el próximo año, ya que los actores sofisticados aprovechan el acceso a terceros para obtener acceso a las redes y los datos de los clientes. Por ejemplo, las empresas mexicanas fueron las que más se vieron comprometidas con sus cadenas de suministro en el ataque registrado al proveedor de software estadounidense SolarWinds, descubierto en diciembre de 2020.[6]

De acuerdo con las tendencias globales, evaluamos además que es probable que los grupos de ciberdelincuentes extorsivos se centren cada vez más en grandes organizaciones en múltiples industrias, en sectores particulares percibidos como vulner-ables a la interrupción operativa, así como en organizaciones que tienen grandes cantidades de datos corporativos confidenc-iales que pueden ser utilizados para obtener más influencia para extorsionar el pago de un rescate.

[3] https://www.wired.com/story/mexico-bank-hack/

[4] symantec-enterprise-blogs.security.com/blogs/threat-intelligence/grayfly-china-sidewalk-malware

[5] https://mexiconewsdaily.com/news/bank-acknowledges-attempted-cyberattack/

[6] https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/

Imagen 3 ▸ Sectores más atacados en México (Enero 2017–Octubre 2021)

Financiero y de seguros	22%
Gobierno	13%
TI y comunicaciones	13%
Energía y servicios públicos	6%
Educación	5%
Manufactura	5%
Petróleo y gas	4%
Farmacéuticos, suministros médicos y salud	4%
Aeroespacial y defensa	4%
Hoteles y entretenimiento	4%
Otros	20%

La cultura de seguridad cibernética débil agrava las amenazas

Junto con el entorno de amenazas externas cada vez más complejo, las deficiencias en las capacidades de seguridad cibernética y su aplicación exacerban los riesgos que enfrentan las empresas con sede en México. A pesar de algunos esfuerzos para mejorar las capacidades y la conciencia del sector público, sobre todo a través de la Estrategia Cibernética Nacional de 2017, el progreso se ha estancado en gran medida desde su adopción, lo que se evidencia en reportes globales como es el Índice Global de Ciberseguridad[7] y el Índice Nacional de Seguridad Cibernética.[8]

A México le fue particularmente mal en la protección de servicios digitales, así como en la respuesta a incidentes y la gestión de crisis. El análisis comparativo del marco mexicano de seguridad cibernética indica además que el bajo compromiso político, la gobernanza limitada de la seguridad cibernética y las deficiencias en los esfuerzos de aplicación de la ley para frenar el ciberdelito obstaculizan la situación.[9] En 2019, el gobierno redujo el financiamiento para adquisiciones de tecnología, lo que generó críticas de los comentaristas locales y algunos sugirieron que los recortes en el financiamiento afectaron la capacidad del país para detectar y responder a los ataques a Pemex y la Secretaría de Economía en 2019 y 2020.[10]

Estas debilidades brindan una amplia base para que una variedad amplia de actores de amenazas cibernéticas, con diferentes capacidades tecnológicas, se aprovechen de las vulnerabilidades de un banco, un comercio o institución en México. Nuestros datos muestran que los actores de amenazas que se dirigen a México se basan en vectores de ataque relativamente poco sofisticados, en particular la ingeniería social, como el phishing. Los informes de código abierto sugieren además que los actores de amenazas que tienen de objetivo a empresas en México, abusan de sistemas mal configurados, versiones desactualizadas de software y vulnerabilidades de aplicaciones. Las violaciones masivas de información personal y credenciales probablemente también faciliten los ataques contra personas y organizaciones en el país, incluso a través del robo de identidad aprovechado para realizar campañas fraudulentas. En términos más generales, la falta de cultura y marcos de seguridad cibernéticos sólidos significa que las entidades del sector privado dependen en gran medida de sus propias defensas y capacidades cibernéticas para detectar, prevenir y responder a los ataques cibernéticos en sus sistemas, así como en los de sus proveedores clave y terceros. Dado el creciente enfoque global en las cadenas de suministro más grandes y en terceros por parte de los actores de las amenazas cibernéticas, esto probablemente representará un desafío clave, incluso para las organizaciones mejor defendidas.

[7] https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

[8] https://ncsi.ega.ee/country/mx/371/#details

[9] https://www.advanced-intel.com/post/latin-america-threat-landscape-the-paradox-of-interconnectivity

[10] https://www.eleconomista.com.mx/tecnologia/Austeridad-de-la-4T-en-tecnologia-afecto-respuesta-a-hackeos-expertos-20200225-0101.html

Estudio de caso: evaluación de amenazas y madurez para una institución financiera con amplia presencia en América Latina

El Cliente se acercó a Control Risks para revisar su capacidad actual de seguridad cibernética, comparar esto con el enfoque de su programa de transformación en curso, y poner las capacidades actuales y futuras en el contexto más amplio del sector financiero.

Los expertos en inteligencia de amenazas cibernéticas de Control Risks y los consultores de riesgos cibernéticos se comprometieron con el cliente en un programa de varios años para proporcionar evaluaciones anuales de su perfil de amenazas y capacidades de seguridad cibernética. Proporcionamos al cliente evaluaciones de amenazas estratégicas en profundidad, junto con escenarios de ataque detallados y realistas, revisando y actualizando al cliente sobre los cambios clave en el panorama de amenazas a lo largo del período. Revisamos el estado de la seguridad cibernética del Cliente, la capacidad y los planes de mejora y los asignamos al marco de control cibernético del Cliente y los estándares internacionales, para identificar brechas en la postura de seguridad cibernética del Cliente.

Nuestro programa de evaluación de amenazas y madurez permitió al cliente evaluar continuamente su progreso en comparación con su estrategia y sus pares, y recibir recomendaciones prácticas en áreas de mejora. Nuestro enfoque basado en amenazas también permitió al cliente priorizar y adaptar sus controles a los cambios en el panorama de amenazas.

De cara al futuro: gestión de riesgos y amenazas cibernéticas en 2022 y más allá

La fragmentación del panorama de amenazas y límites cada vez más difusos entre los riesgos cibernéticos y otros riesgos asociados, incluidos los de reputación, legales, regulatorios y financieros, significa que las organizaciones deben adoptar una visión holística de la seguridad cibernética e involucrar a las partes interesadas de toda la organización en el desarrollo del riesgo cibernético, planes de gestión y respuesta a incidentes.

- La rápida adopción de soluciones digitales en respuesta a COVID-19, y el aumento significativo de conectividad resultante de esto, ha creado vulnerabilidades en las organizaciones que son difíciles de prever. Las organizaciones deben abordar estas vulnerabilidades de manera directa al comprender las posibles nuevas exposiciones y brechas en sus propios sistemas, activos y personas.
- A medida que el entorno de amenazas externas continúa evolucionando, las organizaciones en México deben realizar evaluaciones exhaustivas de riesgos y amenazas cibernéticas para identificar las amenazas y vulnerabilidades clave en sus activos. El monitoreo constante de amenazas tanto cibernéticas como físicas permite a las organizaciones garantizar que sus defensas sean adecuadas para el panorama de amenazas en evolución, mientras que las evaluaciones de riesgo y madurez permiten a las organizaciones comprender mejor sus exposiciones clave y dónde y cómo priorizar la inversión para fortalecer la seguridad cibernética.
- El aumento de los ataques cibernéticos de alto impacto significa que el potencial de impactos sistémicos en una organización, o incluso a nivel nacional, está aumentando. Esto impone mayores exigencias a las organizaciones para que respondan rápidamente a los ataques, y aumenten su nivel de preparación y resiliencia a las amenazas cibernéticas.
- El enfoque activo y creciente hacia las cadenas de suministro tanto de servicios de TI y como de terceros, junto con una mayor dependencia de los servicios digitales, la nube y terceros debido a COVID-19, eleva la importancia de llevar a cabo la debida diligencia cibernética sobre los proveedores clave y la implementación de salvaguardas para la interacción con terceros, así como políticas y protocolos claros para responder a las amenazas en la cadena de suministro.

Sobre nosotros

Control Risks es una consultoría especializada en riesgos que ayuda a crear organizaciones seguras, en cumplimiento y resilientes. Creemos que tomar riesgos es esencial para el éxito, por lo cual proporcionamos la visión e inteligencia necesarias para aprovechar oportunidades y crecer. Nos aseguramos que usted esté preparado para resolver problemas y crisis. Desde la junta directiva hasta la ubicación más remota, hemos desarrollado una capacidad incomparable para traer orden al caos y tranquilidad a la ansiedad.

Ciberseguridad en Control Risks

La oferta cibernética de Control Risks desafía a una industria que generalmente se ha centrado en soluciones técnicas. Creemos que los problemas de seguridad cibernética son principalmente un desafío comercial y estratégico para las organizaciones, y que las organizaciones deben beneficiarse de la digitalización sin preocuparse por la seguridad, integridad y resiliencia de su gente, información y sistemas. Ofrecemos a nuestros clientes experiencia en riesgos comerciales y cibernéticos estratégicos y basados en amenazas.

- **Enfoque de amenazas:** hacemos estrategias que se mantengan relevantes al enfocarse en la defensa contra las amenazas más pertinentes para el cliente y mitigar sus riesgos.
- **Perspectiva estratégica:** damos una perspectiva a los altos ejecutivos sobre los riesgos digitales y tecnológico, antes que los riesgos financieros, políticos y de seguridad más tradicionales que enfrentan.
- **Retorno de la inversión en seguridad:** asesoramos a nuestros clientes para que su inversión en ciberseguridad sea correcta y en función de los riesgos reales, no simplemente en función de los estándares y, a menudo, las mejores prácticas inalcanzables.
- **Experiencia única:** brindamos soporte global integral y de la mano de nuestros clientes, que se basa en más de 40 años de experiencia en consultoría de riesgos.

Los servicios de ciberseguridad de Control Risks

Nuestro equipo cibernético trabaja a nivel global, con hasta 140 analistas de amenazas y riesgos políticos, un equipo de consultores de más de 120 con experiencia en cumplimiento, tecnología e investigaciones y una capacidad de respuesta cibernética global inigualable. Nuestro equipo de inteligencia de amenazas está acreditado en el esquema CBEST del Banco de Inglaterra para la provisión de inteligencia de amenazas cibernéticas a la infraestructura crítica. Tenemos experiencia trabajando en una variedad de sectores, que incluyen finanzas, energía, tecnología, gobierno y telecomunicaciones.

Inteligencia en amenazas

- Análisis y previsión estratégica
- Monitoreo de amenazas
- Suscripción a portal de inteligencia
- Análisis de amenazas remoto y táctico
- Creación de capacidad y diseño de funciones de inteligencia

Proteger

- Consultoría estratégica
- CISO virtual
- Debida diligencia y cumplimiento
- Creación de planes de gestión de crisis y ejercicios prácticos

Respuesta

- Manejo de crisis
- Consultoría en manejo de extorsiones
- Análisis forense tecnológico
- Data Analytics

Oficina de Control Risks en México
Rubén Darío 281
Col. Bosques de Chapultepec
Miguel Hidalgo
11560 Mexico City
Mexico

+52 55 5000 1700
mexicocity@controlrisks.com

controlrisks.com