PERIÓDICO	PÁGINA	FECHA	SECCIÓN
CRÓNICA	PP,6	08/07/2025	LEGISLATIVO

CÁMARA DE DIPUTADOS
LXVI LEGISLATURA
SOBERANÍA Y JUSTICIA SOCIAL

México, ante el desafío de frenar millones de ataques informáticos

Ciberseguridad. Un reporte de la firma estadunidense Fortinet, especialista en protección de sistema digitales, indicó que México encabeza la lista de naciones donde se registraron más intentos de ataques por piratas informáticos en América Latina en todo 2024.

Los sectores más atacados incluyen finanzas, petróleo y gas, telecomunicaciones, salud y servicios públicos, siendo estas industrias las más vulnerables al estar expuestas a amenazas con ransomware, troyanos bancarios y ataques a la cadenas de suministros.

En nuestro país hay leyes para áreas como protección de datos personales, conductas delictivas, telecomunicaciones y seguridad de infraestructura crítica y con ellas se enfrentará a hackers. PAG 6

México, ante el desafío de frenar embates de piratas informáticos

Un reporte especializado señala la espectacular cifra de 324 mil millones tentativas de intrusión individuales en un solo año

Ciberseguridad

Mario Camarillo Cortés
nacional@cronica.com.mx

¿Cómo evitar que los sistemas financieros, industriales y gubernamentales sean blancos de hackers? Estas interrogantes podrían tener en breve una respuesta efectiva con la Ley de Seguridad Pública Federal aprobada el pasado 2 de julio por el Congreso de la Unión, y es que en ésta, se contempla un apartado sobre ciberseguridad, lo que abre una puerta más para blindar los sistemas digitales y contener la artillería de intentos de secuestro de datos en México. Sólo en 2024, estas tentativas sumaron 384 mil millones.

Aunque durante la administración federal pasada se presentaron iniciativas para crear una ley estrictamente enfocada en ciberseguridad, ésta no se concretó. Varios ordenamientos legales abordan aspectos relacionados al tema de manera indirecta e involucran a organismos reguladores que abarcan áreas como protección de datos personales, conductas delictivas, telecomunicaciones y seguridad de infraestructura crítica.

Un reporte de la firma estadunidense Fortinet, especialista en protección de sistema digitales, reportó que México encabeza la lista de naciones donde se reportaron más intentos de ataques por piratas informáticos en América Latina en todo 2024, al registrar el volumen de tentativas de intrusión ya referido. Las principales amenazas incluyen fugas de datos, phishing, ransomware y ataques desde la nube.

De acuerdo con la empresa Infoblox, con sede en Sillicon Valley, California, y especialista en seguridad informática, a nivel empresarial y de Gobierno, los ataques a servicios financieros y contra cadenas de suministros fueron los ciberataques más frecuentes en 2023.

En lo que respecta al factor individual, la principal ciberamenaza en el país se reportó en los fraudes y estafas a través de phishing enviado a través de correos electrónicos, mensajería instantánea y redes sociales con información que buscan engañar a las víctimas para que revelen información confidencial, incluyendo sus claves de acceso.

Un Informe de Ciberamenazas 2024 de la compañía estadounidense SonicWall, subraya que México ocupa el puesto 6 a nivel mundial en ataques a través de correos electrónicos.

En tanto, las compañías de ciberseguridad Fortinet y SonicWall señalan que en México los sectores más atacados incluyen finanzas, petróleo y gas, telecomunicaciones, salud y servicios públicos, siendo estas industrias las más vulnerables al estar expuestas a amenazas con ransomware, troyanos bancarios y ataques a la cadenas de suministros.

Seguridad digital

De acuerdo con la Ciberguía 3.0 del Gobierno Federal, que muestra las herramientas para facilitar la comprensión de conceptos relacionados con la ciberseguridad, en el país existen más de 40 uni-

dades de Policía Cibernética que monitorean posibles intentos de intrusión o amenazas latentes.

Actualmente, dos organismos gubernamentales están a cargo de la ciberseguridad en México: el CERT-MX (Centro de Respuestas a Incidentes Cibernéticos de México) y el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). Se desconoce por ahora si la Secretaría Anticorrupción y de Buen Gobierno, que absorbió todas las tareas del INAI, ya asumió esta tarea en ciberseguridad. Ambos órganos operan bajo los lineamientos generales definidos por la Estrategia Nacional de Ciberseguridad.

Ataques

Uno de los primeros ataques significativos ocurridos en el sexenio anterior, registrado el 10 de noviembre de 2019, hizo de Pemex su blanco. Tres mil computadoras fueron 'secuestradas' por un virus ransomware.

Otro más se registró el 23 de febrero del 2020, cuando la Secretaría de Economía fue atacada por hackers. La dependencia informó que sus servidores e información de sus usuarios no fue vulnerada, sin embargo, se vieron obligados a aislar sus redes y detener operaciones en lo que resolvían el problema.

Entre el 5 y 11 de julio del 2020, la Comisión Nacional para la Protección y Defensa de Usuarios de Servicios Financieros (Condusef), el Sistema de Administración Tributaria (SAT) y el Banco de México (Banxico) fueron blancos de piratas informáticos en sus respectivas páginas de internet y fueron víctimas de ciberataques por el grupo Anonymous México.

Ese mismo año, el Servicio de Administración Tributaria reveló que sufrió un ataque que afectó el funcionamiento de su página de internet, aunque aseguró que la información de los contribuyentes no fue dañada.

En mayo del 2021, la firma de Ciberseguridad Seekurity reveló que el grupo Avaddon atacó por medio de Ransomware a la Lotería Nacional por parte de hackers que se apoderaron de una importante cantidad de archivos que contenían contratos y convenios entre los años 2009 y 2021.

El 30 de septiembre de 2022, los hackers "Guacamaya" vulneraron el sistema de cómputo de la Secretaría de la Defensa Nacional (Defensa), de donde extrajeron información que comprendía del 2016 hasta septiembre del 2022.

En noviembre de 2024, la oficina de asuntos legales de la Presidencia de la República sufrió un presunto ataque de ransomware, de donde presuntamente se extrajeron archivos confidenciales y filtraron datos personales de empleados gubernamentales.

Ciberdelincuencia

En 2025, la ciberdelincuencia elevó su nivel de agresión, varios países son señalados de utilizar a hackers como un arma ofensiva para el ámbito geopolítico y estratégico. Rusia encabeza la lista de quienes lanzan campañas de desinformación, ataques de ransomware y hackeos a centros gubernamentales. Le sigue China, conocida por su avanzada capacidad en ciberespionaje y ataques dirigidos contra instituciones gubernamentales, tecnológicas y militares. Corea del Norte se encuentra en esta lista, al utilizar la ciberdelincuencia como una fuente de financiación de su régimen, con ataques de ransomware, robos de criptomonedas, fraude financiero y robo a bancos

Irán es parte de este grupo, ya que reportes de agencias internacionales indican que ha intensificado sus ataques cibernéticos en respuesta a sanciones y conflictos con EU, Israel y otros países del Golfo Pérsico.

Estados Unidos no es ajeno a este grupo, aunque especialistas resaltan su cooperación contra los ciberdelincuentes, también acapara reflectores, toda vez que sus operaciones suelen tener tintes de espionaje.

En lo que respecta a los países que han sido blanco constante de ciberdelincuentes exitosos (en lo que se extrae información), Alemania encabeza la lista, seguida por Estados Unidos, Francia, España, Irlanda, Italia, Reino Unido, según un reporte de la compañía alemana de seguridad y especialista en informática, Avira.

Otros países europeos también han sido atacados exitosamente por hacker.

Aunque México no figura en el top ten, si destaca por estar entre las naciones donde sus esquemas y sistemas de ciberseguridad no han logrado consolidarse y por tanto garantizar la contención los intentos de intromisión de piratas informáticos que ahora están echando mano de todas las herramientas que aporta la Inteligencia Artificial.

En lo que respecta a los países que han sido blanco constante de ciberdelincuentes exitosos, Alemania encabeza la lista, seguida por Estados Unidos, Francia, España, Irlanda, Italia y Reino Unido

Rusia encabeza la lista de ataques de ransomware y hackeos a centros gubernamentales (de otros países). Le sigue China, Corea del Norte; Irán es parte de este grupo