PERIÓDICO	PAGINA	FECHA	SECCIÓN
La Razón	1-9	09/04/2024	LEGISLATIVO

Víctimas de ciberataque, la mitad de las empresas

Por Sergio Ramírez

REGISTRAN 94 millones de intromisiones maliciosas en 2023; 257 mil diarias; falta de ley y uso de IA facilita fraudes, señalan expertos. pág. 9

Ataques seguirán este año, advierten

Hackeo castiga al país; ahora, apoyado con IA

EMPRESA DE *SOFTWARE* señala que los intrusos informáticos buscan dañar sectores de petróleo, gas, transporte, finanzas...; principal amenaza, fraude y estafa con *phishing*

Por Sergio Ramírez
sergio.ramirez@razon.com.mx

Ante la falta de una ley de ciberseguridad —atorada en el Congreso—, carecer de la cultura de prevención frente a los *hackeos*, y el bajo presupuesto para adquirir tecnología de punta en el sector público, los "ciberdelincuentes" están poniendo en jaque a México, principalmente a empresas y áreas de gobierno, ahora con el uso de Inteligencia Artificial (IA) generativa.

El año pasado, 50 por ciento de las más de 5.5 millones de empresas que, según el Instituto Nacional de Estadística, Geografía e Informática (Inegi), hay en el país, fue víctima de ciberataques, mientras que se registraron 94 millones de intromisiones maliciosas, es decir un promedio de 257 mil 534 eventos diarios.

Datos de FortiGuard Labs, de Fortinet, indican que América Latina y el Caribe sufrieron 200 mil millones de intentos de ataque el año pasado, lo que representó 14.5 por ciento de los ciberataques registrados a nivel mundial. México, Brasil y Colombia fueron las principales víctimas.

EN CUANTO a la inversión pública, México tiene un presupuesto de 45 mil 381 mdp para adquirir bienes y servicios relacionados con Tecnologías de la Información y Comunicación.

Eldato

Aníbal Rojas, vicepresidente de ingeniería en Platzi, plataforma líder en capacitaciones para empresas en seguridad informática y ciberseguridad, señaló que los *hackers* vieron los "beneficios" de la IA y han multiplicado su capacidad de alcance.

"El *phishing* cada vez mucho más elaborado es una cosa que nos preocupa muchísimo, que la gente entienda que esa comunicación tiene que verificarla porque parece que cada vez va a ser más fácil que la gente confunda comunicaciones de origen malicioso con comunicaciones de origen legítimo, que comprometan sus datos personales", declaró a *La Razón*.

Explicó que el *ransomware* (código malicioso que impide la utilización de los equipos o sistemas que infecta) crece de manera gigantesca desde la pandemia de Covid-19 y no ha parado, lo cual afecta a empresas y áreas de gobierno.

criminales de nuevas formas; por ejemplo, al impedir la ingeniería social e imitar las formas de comportamiento humano; es decir, *deep fakes* creados con ella".

Aníbal Rojas, de Platzi, coincidió en el tema al opinar que la IA, además de traer beneficios, también implica riesgos. Añadió que comienzan a emerger dos grandes vectores para el ciberataque: Internet hostings y la Inteligencia Artificial.

El Informe de Ciberamenazas 2024 de SonicWall estableció que la principal amenaza en México es el fraude y la estafa a través de *phishing* enviado vía correos

De acuerdo con Fortinet, empresa de *software*, la tendencia de ataques cibernéticos se mantendrá en lo que resta del año, aunque los delitos no están dirigidos a afectar a individuos, sino a empresas y entidades de gobierno en sectores críticos.

Agregó que los ataques de los *hackers* buscan la obtención de recompensas mayores afectando industrias y sectores como petróleo y gas, transporte, finanzas, agua y servicios públicos, mediante el uso de tecnologías con IA generativa, por lo que cuentan con más herramientas para hacer más sofisticadas las intrusiones digitales.

La compañía alertó que "la Inteligencia Artificial será un 'arma digital' que permitirá a los *hackers* respaldar sus actividades

electrónicos, mensajería instantánea y redes sociales, siendo los más afectados los servicios financieros, con lo que nuestro país ocupa el sexto lugar en el mundo con más ataques a servicios financieros.

Al respecto, la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef) dio a conocer que, en el 2023, los reportes por un posible fraude aumentaron 27.5 por ciento, pues al cierre del 2022 eran 27 mil 373 casos y a finales del año pasado la cifra fue de 34 mil 801 denuncias.

Además, los ciberdelincuentes acechan en la banca móvil, ya que el fraude mediante transferencias electrónicas subió 30.3 por ciento, afectando directamente a más de 27 mil clientes que no reconocen envíos de dinero o movimientos en sus cuentas bancarias.

Dichos fraudes, según la Condusef, provocaron una pérdida económica de más de cinco mil millones de pesos en el 2023, entre usuarios de servicios financieros online o móviles. Lo anterior representa un aumento anual de 49.1 por ciento respecto al 2022, que superaron los tres mil millones.

Fátima Colín, suboficial de la Unidad de Policía Cibernética de la Secretaría de Seguridad de la Ciudad de México (SSC-CDMX), recomendó a los usuarios de la banca no compartir datos personales como nombres, correos electrónicos y números de cuenta a desconocidos.

En entrevista con *La Razón*, indicó que si alguien llega a ser víctima, debe ponerse en contacto con la Policía Cibernética para reportar el enlace o la página, con el fin de recibir asesoría y realizar la denuncia correspondiente.

ATAQUES CIBERNÉTICOS

Fortinet señala que:

VAN DIRIGIDOS A

- Empresas
- Entidades de gobierno en sectores críticos

VAN CONTRA SECTORES DE:

- Petróleo y gas
- Transporte
- Finanzas
- Agua
- Servicios públicos

CASOS

Reportes por posible fraude.

Fuente|**Condusef** Cifras en unidades

RECOMENDACIONES

La Unidad de Policía Cibernética de la SSC-CDMX pide no compartir:

- Nombres
- Correos electrónicos
- Números de cuenta a desconocidos