PERIÓDICO	PAGINA	FECHA	SECCIÓN
EL FINANCIERO	PP-18	12/04/2024	NACIONAL

CIBERCRIMINALES

Dirigen 39% de sus ataques a firmas de energía.

PÁG. 18

PONEN EN ALERTA A LA INDUSTRIA

Cibercriminales dirigen 39% de sus ataques a empresas de energía

Expertos advierten mayor vulnerabilidad de CFE y Pemex, así como en el suministro eléctrico, petrolero y de gas

Este tipo de firmas reciben más del triple de ciberataques que otros sectores

CHRISTOPHER CALDERÓN
ccalderon@elfinanciero.com.mx

Después del sector bancario y financiero, la energía eléctrica y su suministro se han convertido en las industrias con mayor riesgo de ser víctimas de un ciberataque.

Lo anterior, debido a que 39 por ciento de las amenazas lideradas por *hackers* y *hacktivistas* se centran en este negocio, que es considerado como infraestructura crítica, por lo que expertos alertan que la Comisión Federal de Electricidad (CFE) y Petróleos Mexicanos (Pemex) se encuentran en la mira de cibercriminales.

"La digitalización del sector de la energía es una necesidad porque reduce los costos de operación hasta en 25 por ciento o más. Si bien la CFE ha invertido mucho en la digitalización de sus operaciones, esto no significa que está exenta de algún intento de ciberataque o vulneración de sus sistemas", alertó Javier Nava, líder de Movilidad Eléctrica en Hitachi Energy.

Desde 2022, la empresa de ciberseguridad Kaspersky reveló que el grupo Guacamaya, que en ese año filtró información confidencial de la Secretaría de la Defensa Nacional (Sedena), tiene como principal objetivo en México atacar al sector de la de minería, petróleo, gas y energía eléctrica, con el fin de generar daños reputacionales a las empresas e incluso exhibir información que comprometa a las víctimas.

En el pasado, tanto CFE, como Pemex ya han sido víctimas de filtraciones. Tan sólo el 22 de febrero fueron expuestos los datos del sistema de factura electrónica de la petrolera mexicana, que, a finales de noviembre de 2019 sufrió el 'secuestro' de sus computadoras en las oficinas de Pemex en la Ciudad de México.

"Este nuevo *hackeo* (el del 22 de febrero) también dejó expuestos los datos personales de los clientes de Pemex. Esto es muy grave y la empresa debe aplicar medidas de contingencia lo antes posible para proteger a sus clientes; es urgente que nos den cuenta a los ciudadanos de qué está ocurriendo", demandó Víctor Ruiz, fundador de la empresa de ciberseguridad Silikn.

En el caso de la CFE, Silikn estima que, junto a otras 39 dependencias del gobierno de México en las que se incluye a Pemex y a la Comisión Nacional del Agua (Conagua), podría recibir un ataque de *ransomware* que paralizaría sus operaciones.

"Actualmente, la industria de energía tiene un atraso de hasta 15 años en materia de ciberseguridad, lo que hace que las empresas sean vulnerables a múltiples ataques de *phishing* o *ransomware*, este último uno de los más peligrosos debido a que implica el secuestro de información e incluso la suspensión total de las operaciones de una empresa", dijo Víctor Ruiz.

PREOCUPA RED ELÉCTRICA

Según el informe "Ciberataques a infraestructura crítica", elaborado por la empresa de automatización industrial Rockwell Automation, casi seis de cada 10 ejecutivos (57 por ciento) de industrias como la automotriz, manufactura, tecnología de alimentos o construcción ubican a la interrupción de suministro eléctrico como la preocupación más grande frente a un ciberataque.

"Las industrias quieren tener siempre energía disponible para el desarrollo de sus procesos y ante el temor de un ciberataque a las redes eléctricas de CFE, han optado por instalar sistemas de almacenamiento para tener disponibilidad en caso de una interrupción en el suministro e incluso para tener energía cuando esta es más barata", dijo Israel García Palacios, gerente de Administración de Redes en Hitachi Energy.

En este sentido, 90 por ciento de los ejecutivos de industrias esperan que la digitalización de las redes eléctricas en México esté acompañada de una estrategia de ciberseguridad que permita garantizar no sólo el suministro eléctrico, sino también el aumento en la demanda eléctrica que se espera traiga consigo el *nearshoring*.

El reporte de Rockwell Automation advierte que el sector energético recibe más del triple de ciberataques que las verticales atacadas con mayor frecuencia, como es el caso de la manufactura crítica, con 11 por ciento y el transporte, con apenas 10 por ciento de los ataques.

"Las redes eléctricas dependen cada vez más de las tecnologías de la información para manejar, distribuir y almacenar la energía, esto ha ocasionado que estén cada vez más expuestas a robos y secuestro de claves, accesos, manejo de la electricidad, control de la energía, provocación de apagones, desvió de flujos de electricidad, entre otras cosas", señaló García Palacios.

PERIÓDICO	PAGINA	FECHA	SECCIÓN
EL FINANCIERO	PP-18	12/04/2024	NACIONAL

Al cierre de 2023, el *phishing* se convirtió en el ciberataque más común, con 34 por ciento, seguido de los ataques de *ransomware* (secuestro de datos), con 22 por ciento e intrusiones, con 18 por ciento.

Además, el estudio señala que, en el 80 por ciento de los casos, las amenazas provienen de organizaciones criminales rusas, chinas o norcoreanas, mientras que el 20 por ciento de ciberataques restantes son internos, aunque no intencionales al abrir un correo o imagen que permite a los actores de amenaza ingresar a los sistemas de las empresas.

794

MIL INTENTOS
de ciberataques contra firmas de este sector en el mundo se registraron en 2023.

80%

DE LAS AMENAZAS
provienen de organizaciones criminales internacionales de Rusia, Corea del Norte o China.

"Este nuevo hackeo (el del 22 de febrero) también dejó expuestos los datos personales de los clientes de Pemex"

VÍCTOR RUIZ Fundador de Silikn

En el blanco

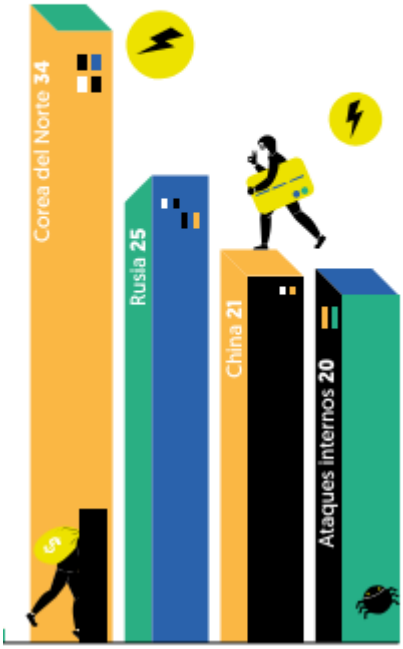
Los grupos que vulneran la información buscan generar daños en reputacionales exhibiendo información comprometedora.

% Ataques dirigidos en México

Extranjeros al ataque

En el 80% de los casos las amenazas provienen de organizaciones criminales rusas, chinas o norcoreanas.

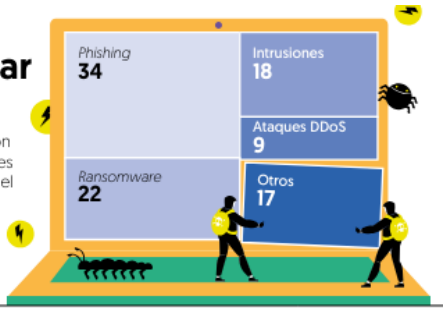
% Origen de ataques por país



Salen a pescar

El *phishing* y el secuestro de datos fueron los ciberataques más comunes el año pasado.

% Tipos de ciberataques a empresas de energía



Fuente: Rockwell Automation y Silikn.