Seguridad y Defensa

7 ciberataques que penetraron los archivos del gobierno de AMLO

Por Esteban David Rodríguez / *EME EQUIS*

Las instituciones del Poder Ejecutivo que fueron objeto de los ataques exitosos son: Pemex, la Secretaría de Economía, la Secretaría de la Función Pública, la Condusef, el SAT, la Comisión Nacional de Seguros y Fianzas, Lotería Nacional y la Secretaría de la Defensa Nacional

Aunque los ciberataques a las instituciones del gobierno federal se cuentan por millones en lo que va de la administración obradorista, se desconoce el total de aquellos que han logrado meter la mano hasta los expedientes y archivos oficiales.

De estos últimos que en efecto penetraron a los repositorios de las plataformas web de la administración nacional, sólo un puñado ha sido revelado a la opinión pública.

Las instituciones del Poder Ejecutivo que fueron objeto de los ataques exitosos son: Pemex, la Secretaría de Economía (SE), la Secretaría de la Función Pública (SFP), la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef), Sistema de Administración Tributaria (SAT), la Comisión Nacional de Seguros y Fianzas (CNSF), Lotería Nacional (Lotenal) y la Secretaría de la Defensa Nacional

Fuera del organigrama presidencial, también hubo ciberataques perjudiciales a otros poderes, como la Suprema Corte de Justicia de la Nación (SCJN) y a organismos autónomos como el Banco Nacional de México (Banxico) y el Instituto Nacional para Transparencia y Protección de Datos Personales (INAI).

2019: EL ATAQUE A PEMEX

En noviembre de 2019, la petrolera estatal fue objeto de un ataque con ransomware del grupo DoppelPaymer. Dicha organización exigió un rescate en criptomonedas: 565 bitcoins, unos cinco millones de dólares.

El gobierno informó que no pagaría. Según Pemex, el ataque de ransomware había sido neutralizado rápidamente y aseguró que no afectó a más del 5% de sus redes.

Tiempo después, en los primeros meses de 2021, la Auditoría Superior de la Federación (ASF) efectuó una evaluación del ataque a la paraestatal. Encontró que en efecto un 5% del equipo informático de Pemex se vio comprometido, pero no era cosa de minimizar, pues los piratas informáticos entraron a 1 mil 816 computadoras.

Publicaciones especializadas aún expresan suspicacias sobre la negativa del gobierno mexicano a pagar el soborno. "Es de suponer que Pemex pagó, pero los representantes de la empresa aún esquivan preguntas sobre el tema", comentó Banamerica en un reporte de 2021.

ATAQUES COORDINADOS

El año 2020 fue exitoso para los hackers que buscaron entrar a los sistemas informáticos del gobierno mexicano.

El 23 de febrero, la Secretaría de Economía detectó un ataque cibernético en algunos de sus servidores. Aunque hubo especulaciones sobre robo de información delicada, el gobierno minimizó el ciberataque y aseguraron de inmediato que no hubo consecuencias mayores, aunque tampoco dieron más detalles.

Lo cierto es que la institución suspendió todos los plazos de los trámites que estaban en curso, tanto para los particulares como para la autoridad. Asimismo, suspendió el plazo para cualquier trámite nuevo que se ingresara de forma física.

Al cabo lo admitió cierto nivel de daño: "Después de realizar una revisión exhaustiva, se identificaron afectaciones en algunos servidores de la Secretaría. Los servicios impactados fueron principalmente los de correo electrónico y servidores de archivos. La Secretaría de Economía ha contado con la colaboración de la Oficina de Estrategia Digital de la Presidencia de la República. Todas las áreas fueron informadas oportunamente para contener posibles afectaciones ulteriores"

En los meses subsecuentes los ataques a instituciones del ámbito financiero continuaron. La Secretaría de la Función Pública (SFP) tuvo un grave ataque al que se refirieron como "accidente de seguridad".

El ataque expuso las declaraciones patrimoniales de 83 mil funcionarios públicos, más de la mitad de los empleados de la administración pública federal, que incluían sus registros federales de contribuyentes y sus claves del registro de población (CURP), y detalles patrimoniales, entre otros datos sensibles. Para julio hubo una nueva serie de penetraciones. Ocurrió entre el 5 y el 20 de julio, y se consideró un "ataque coordinado". A Condusef le quitaron de plano el control de su web. El SAT formó parte de los objetivos de la embestida cibernética, y fue el más hermético en cuanto a los alcances de los daños.

Los ciberpiratas incluyeron entre sus objetivos al Banco de México (Banxico), organismo que no admitió sino "intermitencias".

El 26 de noviembre, la Comisión Nacional de Seguros y Fianzas (CNSF) fue objeto de extorsión cibernética. La cuenta de Twitter de la organización Bank Security difundió que una persona había puesto a subasta los accesos de administración del dominio de la institución del gobierno mexicano, y 10 GB de datos confidenciales de su repositorio. Ese tipo de subastas se hacen en foros de la llamada "red oscura" (dark web), entre delincuentes cibernéticos. La subasta comenzó en 70 mil dólares, según informó Bank Security. El ataque fue en los días posteriores.

Bank Security notificó al Equipo de Emergencia ante Incidentes de Seguridad de UNAM (CERT-UNAM). Pero ni el CERT de la Guardia Nacional ni el de la UNAM lograron reaccionar. El ataque ocurrió el 28, y al día siguiente la dependencia lo hizo público.

2021, AÑO PICO

El ejercicio de 2021 fue uno en el que los ciberataques contra instituciones públicas crecieron. Según reportó la Asociación Mexicana de Ciberseguridad (AMEC), Pemex fue uno de los objetivos principales de los ciberdelincuentes, ya que tan sólo entre enero y junio la petrolera registró 128.8 millones ciberataques. En segundo lugar estuvo la Presidencia de la República, que en el periodo fue objeto de un total de 78.6 millones de embestidas. En tercer lugar, la Secretaría de Educación Pública, con un total de 3.6 millones de eventos.

También fueron objeto de ataques la Secretaría de Salud (14,742); Marina (4,608); el Ejército (1,107) y Economía (15).

Fuera del Ejecutivo, la SCJN recibió 312 mil 716) intentos de penetración; e instituciones autónomas tambien fueron objeto de las andanadas: el INE recibió 2.9 millones de ciberataques; y Banxico (17,669).

Pero de los ataques exitosos que lograron entrar, y que además se comunicaron al público, está el de Lotería Nacional, cuyos sistemas fueron hackeados el 28 de mayo. Los ciberdelincuentes lograron obtener contratos, convenios, finanzas y correspondencia del periodo 2009-2021.

El INAI, organismo autónomo, recibió también una fuerte andanada el 20 de septiembre. concretamente fue la Plataforma Nacional de Transparencia (PNT) comenzó a presentar intermitencias como resultado de ciberataques

Ya en este 2022, la PNT fue objeto de nuevos ataques. Apenas el 11 de julio presentó de nuevo intermitencias como resultado de ciberataques. En consecuencia, los comisionados suspendieron los plazos de entrega de la información. La comisionada Julieta del Río dio a conocer que la plataforma acumulaba 50 millones de ataques en tres días, pero nunca ha sido hackeada.

Con información de www.m-x.com.mx