Elecciones 2021: Advierten riesgo de hackeo al INE y candidatos

Por: Lidia Arista @Lidstelle. Política.Expansión. 10/01/2020

Israel Reyes especialista en ciberseguridad de la Universidad George Washington señala que cibercriminales han sembrado códigos maliciosos en plataformas gubernamentales incluido el órgano electoral.

Primero fueron hackeos a Pemex, a la Secretaría de Energía, al Instituto Nacional de Migración, y **ahora el Instituto Nacional Electoral (INE) está en riesgo en un año clave para la democracia mexicana**, advierte Israel Reyes Gómez, experto en ciberinteligencia electoral y ciberseguridad.

En entrevista con *Expansión Política*, el también catedrático de la maestría de Comunicación Política y Gobernanza de la Universidad George Washington explica que **desde hace varios meses cibercriminales han sembrado códigos maliciosos en plataformas gubernamentales** y hoy está en riesgo el órgano encargado de la organización de los procesos electorales para renovar 15 gubernaturas, 500 diputados federales y centenas de presidencias municipales.

“Encontramos en el *deepweb* y en el *darkweb* información del INE que los compromete hasta cierto nivel… esta información podría ser utilizada para efectuar un ciberataque contra el INE”, detalla.

Reyes Gómez explica que durante la pandemia de coronavirus los ciberataques contra el gobierno de México se incrementaron hasta 900%, y dijo que lo que hace vulnerable de la administración pública es que no solo no está protegida contra el cibercrimen, sino que incluso no sabe que está siendo atacada.

“Cuando estás siendo atacado y no lo sabes, no hay posibilidad de defenderte y creo que ese es el problema de México. Estamos enfrente de un enemigo invisible de quien no sabemos que nos está realizando ciberespionaje”, dice.

Los ataques cibernéticos no son nuevos para el gobierno de México. Hace algunos meses instituciones como la Secretaría de Economía, la del Trabajo, el

Banco de México (Banxico), Pemex, la Comisión Nacional para la Defensa de los Usuarios de Servicios Financieros (Condusef), el Servicio de Administración Tributaria (SAT) y la Secretaría de la Función Pública, sufrieron ataques cibernéticos.

“Son ataques coordinados, primero fue Pemex, después Condusef, al SAT, la Sectur, ha habido una serie de ataques continuos que refleja que hay una coordinación de actores y es el nuevo campo de batalla”, señala.

La bancada de Morena, a través de la diputada Rocío Badillo, propuso castigar hasta con ocho años de cárcel los ciberataques para lo cual planteó tipificar en el Código Penal Federal el delito de sabotaje informático, iniciativa que se turnó a las comisiones donde no ha sido discutida.

El mexicano radicado en Estados Unidos y fundador de la empresa Solity, Israel Reyes, afirma que el INE pueda ser objeto de ataques cibernéticos que podría impactar en el desarrollo del proceso electoral.

¿Cómo puede impactar un ciberataque al INE en un proceso electoral?
El INE ya ha sido víctima de ciberataques, la mayoría no hay sido exitosos porque los han prevenido de una buena manera, pero ellos al no saber qué otra información está comprometida los pone sumamente vulnerables.
El problema es que un ataque bien coordinado, podría ser de riesgo para un instituto electoral, y en un evento donde son las elecciones más importantes de la historia de México tener un ataque cibernético en contra del INE sería devastador no solamente para candidatos, para el gobierno y para el país en general. Hay información del INE, del padrón electoral, de políticos que está a la venta y que va a ser utilizada por opositores y por cibercriminales.

“Los cibercriminales están al servicio del mejor postor y el *deepweb* y en el *darkweb* los es el enemigo invisible porque ahí cualquiera puede pedir que se infiltre a alguien, que le den información sobre un actor político”, destaca.

El experto plantea que **al ser las primeras campañas electorales que tendrán como plataforma de difusión las redes sociales y la vía digital,** los candidatos a gobernador, diputados federales, presidentes municipales y legisladores locales están en riesgo porque estarán en todo momento al acecho de los criminales, quienes podrán incluso hasta vender información a sus opositores.
“Direcciones, correos electrónicos, datos personales, de todo. Esa es la

vulnerabilidad porque uno de los ataques más efectivos porque incluso se pueden robar la personalidad de políticos", refiere.

¿Hay un modus operandi en los ataques a instituciones del gobierno mexicano?
La forma de operar de los cibercriminales es la misma: es a través de correos de empleados, asistentes o proveedores como buscan infiltrarse a las estructuras.

LEER EL ARTÍCULO ORIGINAL PULSANDO AQUÍ

Fotografía: cuartoscuro

Fecha de creación
2021/01/10