Evitando la interferencia en futuras elecciones

En época de elecciones, los gobiernos deben de tomar en cuenta de que hay una gran cantidad de tipos de ciberataques de los que deben de protegerse. Este tipo de **procesos políticos son etapas críticas en cuanto a seguridad informática, ya que aumenta el robo de datos.**

Ataques DDoS, intrusiones maliciosas (defacement), hackeo para cambiar votos o eliminar los mismos, Fake News y publicación de datos sensibles, son algunos de los problemas que deben enfrentar.

Durante la rueda de prensa en la que se anunció la celebración de Infosecurity México 2018, Laura Requena Espada, digital surveillance manager de la firma de ciberseguridad S21sec, dijo que "los datos son el petróleo del siglo XXI", y las estructuras gubernamentales deben de considerar medidas de ciberseguridad para proteger tanto la operación como la información, ya que puede también traer daños a la reputación de los gobiernos y candidatos.

Los ciberdelincuentes han hecho todo lo posible para sabotear procesos electorales en todo el mundo en los últimos años, ya sea a través de campañas de noticias falsas, tambien llamadas fake news, o pirateando directamente los correos electrónicos de los funcionarios.

Es por ello que la compañía española insta a los gobiernos a protegerse ante este tipo de intrusiones.

"Ya se han dado casos, como en las pasadas elecciones de Estados Unidos, en las que se crean sitios web con el objetivo de propagar noticias falsas acerca de los diferentes actores políticos. O un ejemplo más cercano lo pudimos encontrar en un análisis esta misma semana, en la que encontramos un sitio que ofrecía por **un bitcoin la totalidad del padrón electoral mexicano.** Obviamente como compañía no sabemos si esta oferta es real o no, ya que nuestra política es no

realizar la compra, pero el riesgo del robo está ahí", comentó Requena.

Aunque hasta la fecha ningún ciberdelincuente ha llegado a infringir los sistemas de votación en línea de un país y manipular un resultado, se debe de estar pendiente para prevenir este tipo de situaciones.

"El **monitoreo previo y posterior a las elecciones, fortalecer la seguridad de los sistemas**, realizar campañas de concientización de la ciudadanía para reducir la influencia generada por las redes sociales, son acciones puntuales y efectivas para defender la legitimidad del proceso electoral", agregó Requena.