Tanium recomienda reforzar la protección cibernética a instituciones públicas

- Los ataques dirigidos a instituciones gubernamentales aumenta a nivel global.

Ciudad de México. 21 de agosto de 2023.- Tanium, proveedor líder de la industria de administración convergente de terminales (XEM) de la industria, señala que la cantidad de ataques dirigidos a instituciones gubernamentales por la información confidencial que poseen continua aumentando a nivel global. Dada la gran cantidad de datos que parecen estar comprometidos, las personas en el registro electoral, por retomar una muestra crítica, deben tener presente las cada vez más frecuentes actividades fraudulentas, las campañas de phishing que parecen enviadas por el gobierno por correo electrónico, mensaje de texto o de voz, o las redes sociales. Se debe ser especialmente cuidadoso en los detalles del remitente y cualquier enlace antes de hacer clic o responder.

Para Tanium, es preocupante que los datos de un registro electoral puedan contener imágenes personales como copias de actas de nacimiento y pasaportes que posiblemente podrían ser utilizados para fraude. Es poco probable que otros datos se puedan usar por sí solos para causar mucho daño, pero se podrían usar combinados con otra información que un individuo pudo haber compartido en línea de forma voluntaria o no.

El hecho de que los atacantes pudieran tener acceso a una red durante cierto tiempo continuo, es un recordatorio o alerta de que las organizaciones deben implementar prácticas para minimizar la cantidad de tiempo que un intruso tiene para robar información confidencial. Potencialmente, solo le toma unos minutos a un atacante para causar daños, por lo que las medidas de seguridad cibernética correctas son vitales, al igual que el apoyo de organismos locales o mundiales de ayuda cibernética.

Por ejemplo, una de las nuevas medidas de seguridad de la comisión electoral de Reino Unido, es la “capacidad de monitoreo de amenazas”, que es un buen paso, pero solo si tiene una visibilidad completa de sus activos de TI y los dispositivos que se conectan a su red.

“Muchas instituciones del sector público luchan con la visibilidad completa de los endpoints, pero es crucial que tomen el control de todo su entorno de TI para obtener una única fuente de información, de modo que los incidentes puedan investigarse y responderse en tiempo real. Cuando se trata del sector público, algo tan simple como un dispositivo de un empleado sin parchar, puede tener graves efectos secundarios en la sociedad”, señaló Miguel Llerena, Vicepresidente para Latinoamérica de Tanium.