Reto para México, cuidar las fugas de datos y el riesgo del trabajo remoto

- *No hay talento suficiente en seguridad informática y falta resiliencia contra un ataque cibernético.*

Por staff Infosecurity Mexico.

No es de extrañarse que en México cada vez sea más común enterarse de ciberataques dirigidos a instituciones gubernamentales y a empresas privadas de cualquier tamaño, y desde luego, contra las personas. Hay registros[1] de que en 2023 nuestro país recibió 94 mil millones de los 200 mil millones de amenazas que se detectaron en la región de América Latina; de hecho, los intentos de agresiones contra diversas entidades en México representan el 47 por ciento de ataques en LATAM.

De esta situación pudiera surgir una pregunta, ¿qué tan preparado está nuestro país para responder a los ataques cibernéticos? Basta citar algunos ejemplos de esos ataques para darnos cuenta de la situación. Por centrarnos solo en el presente sexenio, el sector público recibió varias embestidas: En noviembre del 2019, Petróleos Mexicanos fue víctima de un ciberataque que afectó al funcionamiento de casi el 5% de sus equipos[2]; en julio del 2021, la Lotería Nacional fue afectada por un ransomware cuyos ejecutores exigían un rescate de 800 mil pesos para liberar la información[3].

En el 2022, la Secretaría de la Defensa Nacional sufrió un primer ataque, de varios; el último, en este 2024, cuando un grupo de ciber piratas puso en venta un subdominio de la institución[4]. En el mismo 2022, la Comisión para la Protección y Defensa de los Usuarios de Servicios Financieros registro un “hackeo” a su sitio web principal. Hacia abril del 2023, la Comisión Nacional del Agua fue víctima de otro ransomware que afectó sus sistemas de información[5]; y así, se han registrado otras invasiones a los sistemas de instituciones oficiales y entidades privadas, y seguramente la lista seguirá, porque los ciber atacantes no descansan.

Sin embargo, uno de los obstáculos para establecer medidas de protección a los sistemas y recursos tecnológicos, es que la ciberdelincuencia está presente en todo el mundo, genera diversas modalidades de ataque y por lo mismo, puede explorar vulnerabilidades una y otra vez, y va modificando sus “armas” de ataque, hasta que logra su objetivo.

Ejemplo de ello son los nuevos ransomwares y malwares descubiertos en mayo de este año en diversas partes del mundo[6]. Son los casos del nuevo malware Lunar, que se usó por ciber piratas rusos para comprometer las instituciones diplomáticas de un gobierno europeo en el extranjero; el nuevo malware para Linux llamado Gomir, creado por el grupo de hackers norcoreano Kimsuki para atacar objetivos en Corea del Sur; o la nueva versión del malware BiBi Wiper que elimina la tabla de particiones del disco para dificultar la restauración de datos. Son solo algunos casos.

Mientras tanto, expertos consideran que México tendrá que atender algunos desafíos mayores en materia de ciberseguridad, como son la supervisión al acceso remoto de los trabajadores, la escasez de talento en seguridad informática, y la falta de resiliencia para responder a un ataque cibernético.

---

[1] https://n9.cl/9yost
[2] https://n9.cl/pl2ijt
[3] https://n9.cl/v7ypw
[4] https://n9.cl/a8wb0
[5] https://n9.cl/xd1es5
[6] https://n9.cl/632sv

Sobre todo porque se calcula que las amenazas más importantes que podrían surgir en nuestro país, corresponden a una fuga de datos, con un 51% de probabilidad; los ataques directos a través de servicios en la nube, con 43%; agresiones a través de desconexiones de trabajadores remotos, con 35% de posibilidad; amenazas avanzadas persistentes, que presentan una probabilidad de 27%; y afectaciones a través de Internet de las Cosas, en la red, con 21%.

Igualmente, vale la pena considerar la posición que tiene México de acuerdo con la clasificación del National Cyber Security Index[7], que elabora un reporte que, entre otros puntos, clasifica el Índice Nacional de Seguridad Cibernética, el cual mide las capacidades de seguridad cibernética de los países con base en las políticas implementadas por los gobiernos centrales; e igual mide el Nivel de Desarrollo Digital, que se calcula según el Índice de Desarrollo del Gobierno Electrónico y el Índice de Preparación para la Conexión en Red.

De acuerdo con este reporte, México se ubica en la posición 39 en el Índice de Seguridad, con 38.33 puntos, y reúne 62.16 puntos en el nivel de Desarrollo Digital. Como referencia, el primer lugar de la tabla del Índice de Seguridad le corresponde a la República Checa, con 98.33 puntos, y la primera posición en el Desarrollo Digital es de Países Bajos, con 84.94 puntos. Cabe señalar que en LATAM, Chile es el país mejor ubicado, en la posición 23 del Índice de Seguridad, con 60.83 puntos, en tanto que Uruguay se posiciona en el lugar 25 de Desarrollo Digital, con 69.19 puntos.

Desde luego, falta mucho por hacer en nuestro país, los retos siguen, y por eso vale la pena asistir a Infosecurity Mexico, en donde los profesionales de la ciberseguridad presentarán varios temas relacionados con la protección de los activos tecnológicos y los bienes informáticos, el 22 y 23 de octubre, en el Centro Citibanamex de la CDMX. Para el efecto, el comité organizador ya abrió registro, incluso el pase gratuito, en el sitio: https://www.infosecuritymexico.com/es/visitantes/pases.html

Facebook: https://www.facebook.com/infosecmexico
LinkedIn: https://www.linkedin.com/company/infosecurity-mexico/
Instagram: https://www.instagram.com/infosecuritymexico?igsh=MWxkeDhzM2Q0N2J3Yw==
Mail de contacto: info@infosecuritymexico.com

[7] https://n9.cl/830t54