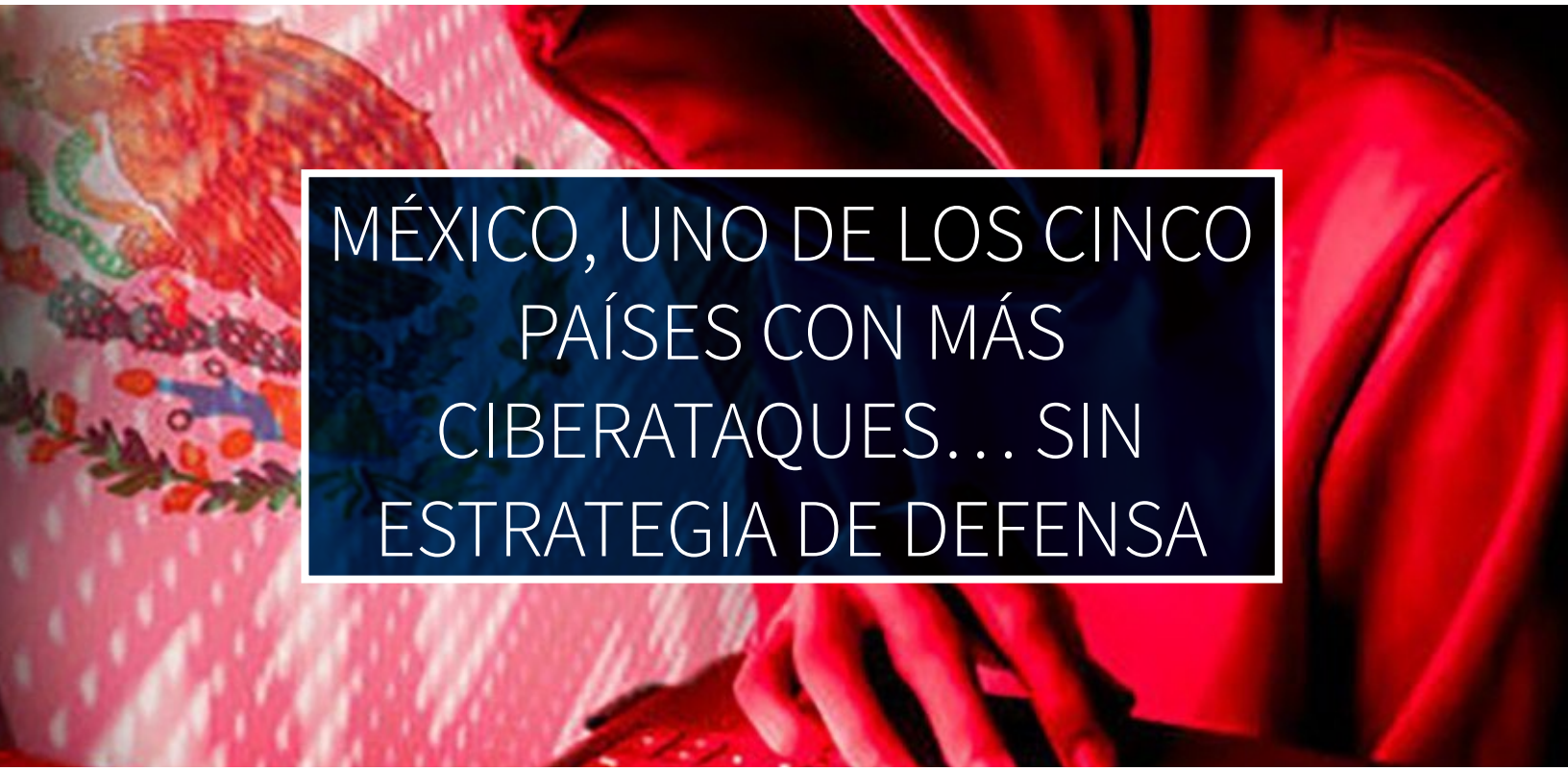
Managed secure IT | no matter what



# MÉXICO, UNO DE LOS CINCO PAÍSES CON MÁS CIBERATAQUES… SIN ESTRATEGIA DE DEFENSA

México está entre los cinco países más atacados a nivel global, sus PyMEs son un blanco importante porque tienen mucha información y poca seguridad, pero faltan estrategias de protección

México se ubica dentro de los cinco países más ciberatacados del mundo, y ello se debe en gran parte a la ignorancia de los usuarios hacia las amenazas que existen, tanto a las computadoras a los servidores y a los dispositivos móviles, afirmó Fernando Thompson de la Rosa, director general de TI en la Universidad de Las Américas Puebla durante la presentación del panorama de ciberamenazas organizado por Infosecurity Mexico 2019.

Ese mismo desconocimiento también es de los altos directivos de empresas y funcionarios de gobierno, que no destinan inversiones suficientes para disminuir este problema, y por eso no cuentan con herramientas avanzadas ni personal especializado, comentó el ejecutivo.


Para el encargado de TI en la UDLAP, las instituciones y corporativos deberían destinar por lo menos el 10% de su presupuesto a cuestiones de seguridad, tanto en hardware como en software, además de capacitar y certificar a su personal encargado de esa materia, aunque el problema es que tal práctica es escasa.

“Sabemos que, en nuestro país, cerca del 90% de empresas que impulsan nuestra economía son PyMEs, pero también son presas de ciberataques porque representan un blanco muy atractivo ya que tienen bases de datos con información de sus clientes, además de datos financieros y contables, y por ello pueden sufrir hasta (secuestros) de sus servidores”, añadió Thompson.

Para lo que resta del presenta año, el ejecutivo visualiza que aumentarán los ataques relacionados con la minería de datos, al igual que el ransomware, ya que 82% de los ataques por internet (82%) son ataques de código malicioso, cuyo objetivo en general es el robo de datos.

“Eso afectará a los usuarios comunes y al sector empresarial, independientemente del tamaño de la empresa. Por ello debemos mejorar la cultura de ciberseguridad a través de la capacitación y cuidar acciones como la revisión de correos, cuidarse de no navegar en sitios de dudosa procedencia, estar alerta ante el pishing, y no dar clic a ligas desconocidas. Creemos que el usuario final representa el eslabón más débil y por ello hay que diseñar estrategias de información y de educación hacia todos los niveles y en todo tipo de instituciones”, indicó.

Thompson explicó que la realidad en México indica que las PyMEs no cuentan con el conocimiento ni con los recursos suficientes para conformar una eficiente área de seguridad, la cual generalmente recae en el administrador de la red o de las aplicaciones de negocios. A cambio, hay atacantes con conocimientos y que usan herramientas avanzadas para atacar tanto a pequeñas como a grandes empresas. Por ello es que todas las organizaciones requieren de especialistas en seguridad que entiendan lo que sucede en el mundo actual.

Crecen las ciberguerras y se requiere estrategias de seguridad de estado

Más allá del ámbito empresarial; el entorno mundial está enmarcado por ciberguerras que empezarán a afectar a todos los países. Hay herramientas tecnológicas que se están adaptando a las necesidades de ciberseguridad, incluso a nivel mundial, como son la inteligencia artificial y el aprendizaje automático (machine learning). Se trata

de un par de herramientas muy valiosas porque pueden manejar una multitud de variables que el ser humano no puede controlar por sí solo.

Sin embargo, debido a que esas tecnologías serán cada vez más accesibles a un mayor número de mercados, esas mismas herramientas son igualmente utilizadas por el cibercrimen. Por eso las organizaciones deben ser capaces de adaptar un esquema de seguridad flexible, dependiendo del evento que se lleve a cabo en ese momento; si están captando una variante de ransomware, en ese momento van a tener que definir una postura para decidirse por la contención y luego por la erradicación.

El ejecutivo verbalizó que los criminales actuales son capaces de espiar llamadas telefónicas, correos electrónicos, mensajes en redes sociales y dispositivos de ciudadanos porque saben que la información es poder y le resulta redituable, además de que casi no se detiene a los responsables de estos delitos. Para Thompson, la figura del hacker solitario quedó atrás: “Hoy debemos cuidarnos de verdaderas organizaciones que usan tecnología de punta, tienen muchos recursos y están organizados para cometer crímenes en línea.

Sin embargo, vemos que la ciberseguridad no es una prioridad en la agenda de la presente administración, pero el gobierno debe darse cuenta que no puede actuar solo, sino que debe trabajar en conjunto con la iniciativa privada e incluso con otros países, porque se trata de estrategias con resultados a mediano y largo plazo. Se tiene que actuar ya”, concluyó el experto.

Fuente:
*https://searchdatacenter.techtarget.com/*

## Síguenos en nuestras redes sociales:

MexisMX

Servicios Administrados Mexis, S.A. de C.V.

Mexis TI

Servicios Administrados Mexis, S.A. de C.V.