La Ciberseguridad en México

By Redacción on Mié, 05/05/2021 - 14:19
Por Adriana Guzmán, Directora Ejecutiva en Brand PR Digital

De acuerdo con la Organización de las Naciones Unidas (ONU), en el mundo ocurre un ataque informático cada 39 segundos y México ocupa el tercer lugar global en ciberataques, tan solo el 13.2% de las empresas han sido víctimas de ataques cibernéticos.

Ninguna empresa es inmune a un ataque de este tipo. La inquietud no reside en saber entonces si existe la posibilidad de que les pase, sino en cuándo va a sucederles.

La buena noticia es que México también se encuentra entre los tres países más desarrollados en temas de ciberseguridad en América Latina. Nuestro país está llevando a cabo diversas iniciativas en esta materia, tanto en el sector privado como en el público.

“La ciberseguridad es un tema que llegó para quedarse y, en ese sentido, las organizaciones deben no solo desarrollar sus capacidades para ser una empresa más “segura” sino también de “vigilancia” y “resiliencia”, es decir, ser capaces de anticiparse al impacto que una amenaza pueda implicar progresando en capacidades de ‘ciberinteligencia’, y reaccionar correctamente cuando el incidente se manifieste”. Comenta Jesús Navarro, Director General de Data Warden, empresa 100% mexicana dedicada a salvaguardar los datos, información y transacciones de las empresas

La pandemia provocada por la SARS-CoV-2 obligo a las empresas a nivel global a enviar a sus colaboradores a casa y con ello, quedó expuesto un perfil atractivo para los ciberdelincuentes. El home office llevó a algunas empresas a coordinar acciones con sus colaboradores quienes emplearon sus propias laptops, con el único propósito de dar continuidad a sus negocios. Entre los principales incidentes de seguridad informática en tiempos de Covid-19, Navarro resaltó ataques ransomware y suplantación de identidad mediante phishing.

Pero ¿qué se puede hacer para que las empresas puedan salvaguardar su información, datos y transacciones? La estrategia que recomienda el especialista en ciberseguridad consiste en contar con Asesoría Especializada para la evaluación, planeación y ejecución de controles de seguridad para los activos tecnológicos de la organización, por medio de la identificación, reducción de riesgos y amenazas que afecten su confidencialidad, integridad y disponibilidad. Establecer dentro de la empresa la Arquitectura Tecnológica adecuada, para implementar soluciones robustas de ciberseguridad. Y Contar con una Adecuada Operación de ciberseguridad para proteger los activos de los clientes en el día a día, mediante un enfoque de detección y respuesta efectiva y oportuna ante amenazas cibernéticas.

En el libro “Ciberseguridad para Ejecutivos: Una guía orientada a minimizar los riesgos y comprender las nuevas amenazas de la década”, se plantean los nuevos retos y los desafíos que deberán afrontar las empresas en los años por venir. El libro realizado entre Data Warden en colaboración con el Dr. José Luis Cisneros, Director de TI de Casa de Bolsa Finamex, representa una guía para ayudar a los ejecutivos tomadores de decisiones a salvaguardar los datos, información y transacciones de sus empresas, además de generar conciencia de seguridad con el público en general.

En días recientes Data Warden presentó su nueva imagen que consiste principalmente en lograr una mejor presencia de marca, con el rediseño de su logotipo, nuevas instalaciones, la actualización del sitio web el cual luce más corporativo, sencillo e intuitivo para navegar, y la presentación de Kahu que es el personaje icónico de la marca cuyo nombre significa “guardian” en hawaiano, y hace referencia al casco de un guerrero que cuenta con tres armas, una lupa “White” que ayuda a detectar amenazas, un escudo “Blue” para dar protección y blindaje y un hacha “Red” para luchar contra los ataques cibernéticos.

La ciberseguridad se ha convertido, sin lugar a dudas, en un problema para el negocio de una compañía y no solo para su área de tecnología; es un tema cada vez más presente entre los consejos de administración, los comités de auditoría y directivos de las organizaciones.

En cuanto al futuro este fenómeno seguirá sucediendo mientras las empresas continúen abriéndose al mundo digital, una tendencia que no va a parar y que se ha impulsado con iniciativas como el Internet de las Cosas, que ha engrandecido el terreno sobre el cual hoy los atacantes actúan.

“En ese sentido y para lograr un mejor futuro las organizaciones deben aprender a mejorar sus niveles de protección, detectando cuáles son las áreas en donde

necesitan invertir más tiempo, dinero y esfuerzo para protegerlas de forma eficiente", comenta Navarro.