Hackers mexicanos son de los mejores del mundo, dice Stefan Leipold

De visita en México para anunciar su nuevo libro, el emprendedor serial y experto en tecnología habla en exclusiva con Tech Bit

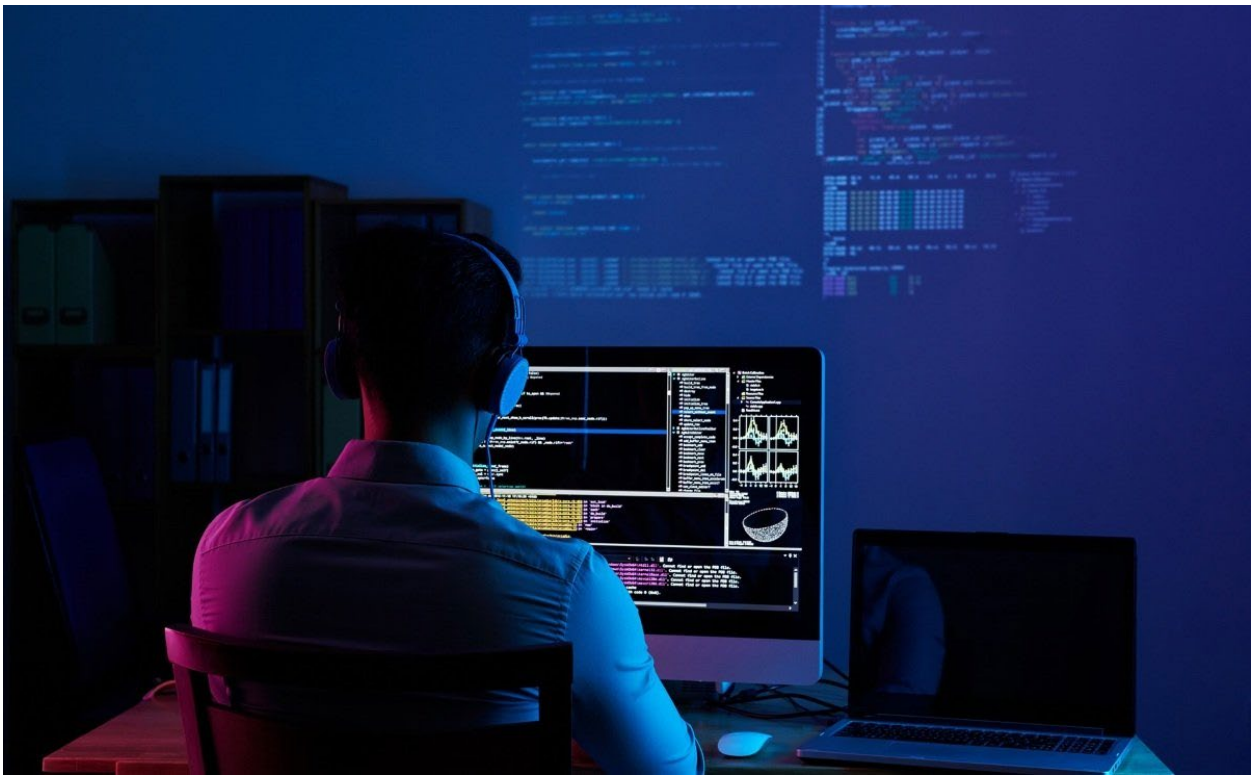

Imagen: Pixabay

Techbit 31/08/2021 00:05 Octavio Castillo Actualizada 00:05

A nivel **ciberseguridad**, México cuenta con una dualidad interesante: es al mismo tiempo uno de los países con los mayores niveles de vulnerabilidad y, una de las naciones con mayor potencial para el **hackeo ético**.

Este es el diagnóstico que **Stefan** Leipold, CEO y fundador de **Stark LLC** y **ProSysCo**, empresas enfocadas en la **seguridad informática** y con quién **Tech Bit** tuvo una charla exclusiva.

De acuerdo con el experto en **ciberseguridad**, en general, las **empresas mexicanas** cuentan con muy pocos protocolos e infraestructura dedicada para la ciberseguridad. Por otro lado, la

tecnología relacionada con este tema que se encuentra desplegada ya está desactualizada o tiene poco mantenimiento.

“Hace unas semanas me hospedé en un hotel de **Reforma** y pude conectarme desde su red **Wi-Fi,** con mi teléfono, a su sistema. Pude ver, incluso, la información de los huéspedes y otros datos de la **computadora** de recepción. Le tomé capturas de pantalla y les dije: pasen estas imágenes a sus equipos de IT para que mejoren su seguridad. Algunas semanas después volví al mismo hotel y no habían mejorado ni una sola de sus medidas de **seguridad**”.

Stefan **Leipold** asegura que incluso en el caso de que una empresa sea atacada y logre recuperarse sin perder información, esto no significa que los **ciberdelincuentes** los dejarán por la paz, sino todo lo contrario.

El libro "La decisión" trata sobre cómo Stefan Leipold pasó de vivir en la calle a ser un empresario tecnológico exitoso

“En casos, como por ejemplo, de **ransomware**, los cibercriminales pueden encriptar todos los datos de una empresa y dejarla inoperativa. La solución más sencilla, que muchas compañías realizan, es pagar el “**rescate**” de la información. Sin embargo, aun cuando recuperen los datos secuestrados, esto vuelve a las empresas “clientes” de los **delincuentes**. Es decir, con la llave para recuperar la información, luego de pagar el rescate, normalmente viene un mensaje que dice: tienes 30 días para mejorar tus **sistemas** de **seguridad** porque te vamos a volver a atacar. La razón de esto es porque las empresas pagan”.

El experto en seguridad asegura que el “**home office**” implementado por las empresas durante la pandemia **agravó** la **vulnerabilidad** de las organizaciones a nivel global.

“La implementación del trabajo remoto tiene a un gran número de personas trabajando desde casa, utilizando **conexiones** de **red** poco fiables. En muchos casos desde la misma computadora de casa desde la cual el esposo o la esposa trabajan, los hijos navegan en Internet de formas poco seguras. Esto incrementa el riesgo para las empresas ya que cuando se deciden a implementar **infraestructura** para la seguridad piensan siempre en el corporativo físico. Hay pocos o nulos elementos que protejan los **equipos** de **cómputo** portátiles, los **teléfonos inteligentes** o las conexiones”.

Pandemia impulso transformación digital

Stefan **Leipold** asegura que un efecto positivo de la pandemia de **Covid-19** fue que obligó a las empresas a iniciar sus proyectos de **transformación digital**.

“En el caso de **México** es notorio cómo el tema del trabajo desde casa detonó muchas iniciativas de **transformación digital**. Eso es algo positivo. Poco a poco comienza a verse el tema de la **seguridad** como una de las prioridades para la operación de un negocio. Muchas empresas se vieron en la necesidad de implementar **tecnología** para mantenerse funcionando, el siguiente paso para muchas es garantizar la seguridad de su operación”.

Las empresas de **Leipold** no solo proveen de asesoría a las organizaciones que requieran un análisis de su situación de **seguridad informática**, también desarrollan productos para mejorar la **privacidad** de la información. Entre ellas se encuentran las pantallas de privacidad adheribles a **teléfonos inteligentes** y **laptops** que evitan que la pantalla pueda ser vista por nadie además de la persona que las está usando.

“Son removibles, se pueden lavar y poner de nuevo, no permiten a nadie que se encuentre al lado poder ver el contenido de la **pantalla**, es una manera muy eficiente de evitar que personas malintencionadas tomen fotografías o memoricen datos de tarjetas de crédito cuando se hacen **compras en línea** o puedan acceder a información confidencial cuando por ejemplo, en un viaje de trabajo, la persona está dando los toques finales a una presentación en la computadora”.

Algo que **Stefan Leipold** encuentra positivo en **México** es el gran potencial para **hackeo ético** que existe en el país y que no se ha explotado como un servicio que podría tener alcances globales.

“México tiene muy buenos **hackers**. Quienes se dedican a ello son muy buenos, independientemente de que se dediquen a cosas ilícitas o no. Aquí he encontrado un gran talento que no está siendo aprovechado. Con la dirección adecuada, los **hackers mexicanos** podrían estar entre los mejores del mundo dando consultoría a las empresas, **hackeando** y rompiendo sus sistemas para ayudar a encontrar **vulnerabilidades**. Es algo que no se dice mucho cuando hablas de ciberseguridad en el país, por ello me parece importante señalarlo: México tiene hackers entre los mejores en el mundo”.

También te puede interesar: Cómo calibrar la batería del celular para que dure

Temas Relacionados

ciberseguridad Hackers