Es importante proteger tu negocio

Desde hace varios meses, muchas organizaciones y empresas realizaron diversas acciones con el objetivo de hacer más eficiente el trabajo desde casa, una situación que fue inevitable debido a la contingencia sanitaria mundial.

En dicho contexto, cabe preguntarse ¿cuáles son las implicaciones a largo plazo de este flujo de trabajo desde el punto de vista de ciberseguridad? ¿Qué pueden hacer las empresas para que los empleados y la información confidencial esté protegida?

Con el distanciamiento social y el uso de equipos de trabajo diferentes a los ubicados en las oficinas, los empleados pueden utilizar sus teléfonos portátiles para consultar el correo empresarial, conectarse a redes Wi-Fi domésticas o de libre acceso, por lo cual pueden quedar expuestos a ataques debido a la falta de protección profesional.

Según el informe de Netscout “Threat Intelligence Report” en el 2020 se realizaron más de 10 millones de ataques DDoS (Distributed Denial Of Service) en un año. Estos ataques DDoS son una de las amenazas más famosas realizadas a través de dispositivos móviles, junto con el ransomware, y perjudican la productividad, el servicio al cliente y reducen las ventas de las empresas.

En el caso específico de América Latina, la frecuencia de ataques cibernéticos incrementó en un 50%, donde México ocupa el cuarto lugar de un top cinco conformado por Brasil, Chile, Colombia y Perú. Según cifras del Sondeo de Seguridad Empresarial realizado en nuestro país, el 13.2% de los encuestados reportaron que sus empresas fueron víctimas de este tipo de ataques.

Para gestionar estos problemas, las empresas utilizan tecnologías como CASB (Cloud Access Security Broker) y SASE (Secure Access Service Edge), tendencia que continuará acelerándose junto a la digitalización de las compañías.

En este sentido y de acuerdo con el Digital Trust Insights 2021 de PwC, el 53% de las empresas tendrá una digitalización acelerada para impulsar el crecimiento de sus negocios y 56% pondrá a la ciberseguridad al centro de sus decisiones.

Con esta prioridad en mente, es importante delinear una estrategia enfocada donde se consideren diversos aspectos como la capacitación del equipo de tecnología de la compañía, el establecimiento de protocolos de acción ante posibles ataques y la adquisición de un software adecuado para la gestión de datos; de esta manera, se podrá garantizar la seguridad de la empresa y de los mismos clientes.

Fuente:

Estrategia de ciberseguridad en México: retos para un futuro ciberseguro.https://expansion.mx/tecnologia/2020/12/03/estrategia-de-ciberseguridad-en-mexico-retos-para-un-futuro. 3 de diciembre de 2020.