

¿Tu empresa está preparada para detener un ciberataque?

Ciudad de México, 22-10-2021 |

Autor: Agencia NotiPress

Detección oportuna de una amenaza digital es clave para reducir los daños a la organización afectada

Empresas de todo el mundo almacenan información como cuentas bancarias, clientes, documentos legales y otros, representando su principal activo. Bajo este contexto, los ciberataques que van tras ellos perjudican seriamente a la organización ocasionando daños millonarios. Esta situación exige un esfuerzo colectivo, con especial hincapié en las nuevas estructuras de ciberseguridad y el uso responsable de tecnologías.

Un ciberataque puede representar un golpe duro para cualquier empresa en términos económicos y de credibilidad, aseguran expertos. En entrevista exclusiva para NotiPress, Jesús Navarro, CEO de Data Warden, empresa especializada en seguridad informática, comentó que la ciberseguridad debe ser pilar para cualquier organismo y así se demostró en tiempos de pandemia. "La apertura de canales digitales requiere habilitar mecanismos de trabajo que antes no estaban disponibles. Con el trabajo remoto, hay empresas que se están dando cuenta que no tenían la estructura para hacerlo y ahora se enfrentan a problemas gravísimos que representan un gasto mayor al de preparar una estrategia de seguridad previa", indicó Navarro.

A nivel mundial, el 82% de las empresas manifestaron su preocupación entorno a los riesgos de seguridad digital, de acuerdo con el reporte 2021 Thales global data treath. El estudio señala que el 41 por ciento de ellas experimentaron ciberataques en el último año. Las principales amenazas están relacionadas con ransomware, "secuestro" de información en el que un malware encripta archivos y pide un rescate para desbloquearlos. El phishing: roba información como contraseñas o datos bancarios a través de la suplantación de identidad. Por último esta el



criptominig y se da cuando un dispositivo es infectado por un sistema capaz de producir y extraer criptomonedas sin ser detectado.

Desde Okta, plataforma que trabaja en simplificar la administración tecnológica de empresas, señalan que hay una gran variedad de formas prevenir y enfrentar un ciberataque. "Hay que estar consciente de que un ciberataque es algo real y le puede suceder a cualquier empresa. Es necesario poner atención a la autenticación de datos, saber quien pertenece a la empresa, y asegurarnos que lo haga de forma segura. Lo ideal es que no sea un plan momentáneo, sino un programa constante con actividades puntuales y priorizadas", recomienda Todd Mckinnon, CEO y cofundador de Okta.

En este sentido, Ernesto Rosales, director de servicios administrativos de Data Warden, señala que los pasos para prevenir y gestionar un ciberataque tienen diferentes fases: prevención, detección y recuperación. Es importante definir roles y niveles de acceso a la información, tomando como pilar las buenas practicas para la gestión de datos. El momento en el que se detecta un ciberataque es crucial, pues una buena gestión representa una reducción significativa del impacto. Las principales medidas en esta fase son técnicas y de organización con una continua monitorización de la arquitectura digital. Para la recuperación se recomiendan tácticas de restauración de datos, tales como backups y copias de seguridad.

La ciberseguridad es un tema complejo y cambiante debido a que está ligado a los avances tecnológicos y la evolución de ciberataques. Su importancia radica especialmente en la necesidad de evitar consecuencias negativas en todas las áreas de una empresa. "El problema es que se ve a la ciberseguridad como algo que no genera un retorno de inversión claro o que no tiene un valor estratégico. Es necesario revertir esta situación y que no se tome como un gasto innecesario sino como un habilitador de negocio. Mientras más seguridad tengas, más confianza tendrán tus usuarios", recalca Jesús Navarro.

