

Extorsiones por ataques DDoS en LA cuestan a las empresas 150 mil dólares al día: Arbor

Arbor Networks, la división de **seguridad** de **Netscout**, calcula que cada día las empresas en Latinoamérica pagan alrededor de 150 mil dólares por **extorsiones** relacionadas con **ataques de denegación de servicio (DDoS)** tomando en cuenta que cada 6 segundos se genera un ataque de estas características en la región.

“Hoy por hoy la seguridad forma parte del negocio, la existencia o la carencia de la misma. Las estructuras organizacionales modernas lo entienden mucho mejor, **la seguridad es una área totalmente independiente que forma parte del negocio**, hasta que no entendamos eso va a ser difícil tener soluciones; la gente de seguridad debe tener la misma importancia que áreas como marketing, ventas, finanzas, comercial”, comparte Daniel Villanueva, Vicepresidentes de Ventas para Arbor Networks en Latinoamérica.

El monto compartido no toma en cuenta los demás **costos asociados por la pérdida del servicio**, las comunicaciones no completadas o el tiempo extra y aplicación de **recursos adicionales** por las áreas de TI, independientemente del **daño a la reputación** que ser atacado puede desencadenar como la pérdida de nuevos clientes y nuevos negocios, y las **penalizaciones** que pudiera imputar la autoridad.

Lo anterior fue compartido por Villanueva en el marco del evento ¿Es momento de reevaluar su riesgo ante **ciberamenazas de DDoS?**, organizado por la compañía en colaboración con la **Oficina Comercial de la Embajada de los Estados Unidos en México**.

Juan Luna, Director General de Arbor Networks en México, compartió que el **tamaño de los ataques DDoS** detectados en el país ya superan los 100 Gbps, 67% de los cuales son **multivectoriales**, es decir utilizan distintos métodos de manera simultánea para saturar el **ancho de banda** y generar un agotamiento de estado en la **infraestructura**, “estas amenazas se utilizan porque son difíciles de contraatacar ya que las empresas no tienen infraestructura dedicada para la **detección** y **mitigación** de estos ataques”, concluye.