TECNOLOGÍA | SEGURIDAD INFORMÁTICA

**Pese a la reducción del riesgo de ataques, organizaciones anticipan hackeos en 2023**

*El Índice de Riesgo Cibernético de Trend Micro muestra una mejora gradual en la preparación. A pesar de la disminución del riesgo, el 78% de las organizaciones prevé ataques exitosos en 2023.*

**Por Julián M. Zappia.  
Diplomatic Week.**

El vicepresidente de inteligencia de amenazas de Trend Micro, Jon Clay, informó que el índice de riesgo cibernético mundial ha mejorado por primera vez, indicando que las organizaciones están tomando medidas para mejorar su preparación. Sin embargo, los empleados siguen siendo una fuente de riesgo.

La preparación cibernética ha mejorado en Europa y APAC, pero ha disminuido en Norteamérica y Latinoamérica. Las amenazas han disminuido en todas las regiones, excepto en Europa.

A pesar de estas mejoras, la mayoría de las empresas son pesimistas sobre el próximo año, con un 70% y 69% de los encuestados esperando una brecha en los datos de los clientes y la propiedad intelectual, respectivamente, y un 78% anticipando un ciberataque exitoso.

Las principales amenazas identificadas fueron el clickjacking, el compromiso del correo electrónico empresarial, el ransomware y los ataques sin archivo. Los empleados negligentes, la infraestructura de cloud computing y los empleados móviles/remotos fueron identificados como los principales riesgos de infraestructura.

Los encuestados de todo el mundo también mencionaron a los empleados como tres de sus cinco principales riesgos de infraestructura:

* Empleados negligentes.
* Infraestructura y proveedores de cloud computing.

* Empleados móviles/remotos.
* Escasez de personal cualificado
* Entornos informáticos virtuales (servidores, endpoints, etc.)

Las empresas están preocupadas por la falta de visión de la seguridad como una ventaja competitiva, la incapacidad para desencadenar contramedidas y la falta de conocimiento de la ubicación física de los activos de datos y aplicaciones críticas.

Para minimizar los riesgos, las empresas deben aplicar las mejores prácticas de seguridad, incluyendo la identificación y protección de los datos críticos, la implementación del descubrimiento de la superficie de ataque, la minimización de la complejidad de la infraestructura y la inversión en talento. También deben revisar las soluciones de seguridad existentes y mejorar la arquitectura de seguridad de TI.

El Índice de Riesgo Cibernético semestral se basa en entrevistas con 3.729 organizaciones mundiales y se calcula restando la puntuación de las ciberamenazas de la puntuación de la “ciberpreparación”.