

Cinco principales amenazas de ciberseguridad para 2024

78% de las empresas clasifican la seguridad/fugas de datos como la principal causa de inactividad no planificada de servidores y aplicaciones.

No te dejes sorprender desprevenido.

1

Seguridad en la cadena de suministro: Amenazas en aumento



Cuanto más proveedores tiene una organización, independientemente de su tamaño, más amplia es su superficie de ataque a lo largo de la cadena de suministro.

50% de las organizaciones encuestadas trabajan con más de 1.000 proveedores.²

98% de las organizaciones encuestadas han sido impactadas negativamente por una violación de seguridad cibernética en su cadena de suministro.³

Para estar preparado, elija un proveedor que:

- ✓ Tenga un ciclo de vida de desarrollo seguro.
- ✓ Use logística segura durante el envío para proteger contra manipulaciones.
- ✓ Mantenga un programa de proveedores de confianza.
- ✓ Posea y controle su manufactura.
- ✓ Tenga una cadena de suministros reconocida en la industria con una iniciativa de resiliencia de la cadena de suministros.

Ataques "por debajo del SO": Una amenaza creciente a reconsiderar



2

El firmware "por debajo del SO" a menudo se pasa por alto, pero es un área de enfoque creciente para los atacantes.

Más del 80% de las empresas han sufrido al menos un ataque de firmware en los últimos dos años.⁴

¿Soluciones potenciales?

- ✓ Elija un proveedor con un programa de seguridad robusto que ofrezca evaluaciones proactivas de seguridad de firmware y actualizaciones oportunas de seguridad de firmware.
- ✓ Monitoree, asegure y actualice regularmente el firmware del servidor para detectar y proteger contra manipulaciones.
- ✓ Seleccione productos con capacidades de seguridad de firmware/hardware como arranque seguro (por ejemplo, Intel® Boot Guard/AMD® Secure Boot) y una raíz de confianza de resiliencia de firmware de plataforma compatible con el NIST SP 800-193.

3

Encontrando los proveedores adecuados: Elija transparencia



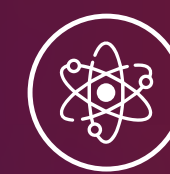
Un proveedor que ofrece transparencia a lo largo del ciclo de vida del producto puede brindar la tranquilidad de que sus datos — y los de sus clientes — están seguros.

Líderes en cadena de suministros que incrementaron la visibilidad de extremo a extremo en sus cadenas tuvieron el doble de probabilidad de informar que no enfrentaron desafíos por impactos en la cadena de suministros en 2022.⁵

Para estar preparado, elija un proveedor con transparencia de extremo a extremo mediante herramientas como:

- ✓ Atestaciones de evaluaciones de seguridad de terceros
- ✓ Asesoramientos de equipos de respuesta
- ✓ Firmware descriptado y descargable gratuitamente
- ✓ Capacidades como la Cadena de Suministros Transparente de Intel®

Computación cuántica: Impulsando cambios en la encriptación



4

La computación cuántica hará inseguros la mayoría de los métodos actuales de cifrado asimétrico.

Más del 50% de los profesionales encuestados creen que sus organizaciones corren riesgo de ataques de ciberseguridad del tipo "recoger ahora, descifrar más tarde".⁶

¿Soluciones potenciales?

- ✓ Utilice sistemas y aplicaciones que admitan algoritmos resistentes a la computación cuántica hoy.
- ✓ Elija proveedores que respaldarán algoritmos post-cuánticos a medida que se consoliden los estándares.

5

Amenazas de ransomware: Todavía un problema



Aunque el ransomware no es un nuevo riesgo de ciberseguridad, sigue siendo una amenaza que continúa demandando atención.

25% de todas las brechas en 2022 involucraron ransomware.⁷

Más del 130 variantes diferentes de ransomware se han detectado desde 2020.⁸

¿Soluciones potenciales?

- ✓ Implemente soluciones de gestión de datos con autenticación de usuario resistente a ataques.
- ✓ Implemente soluciones de disponibilidad de datos para asegurar que pueda restaurar rápidamente los activos después de un ataque.
- ✓ Utilice soluciones de almacenamiento con protección integrada contra ransomware.

Su infraestructura principal podría estar en riesgo.

Asegúrate de estar preparado.



Para más información:

Conéctate con una cuenta de Lenovo o un representante de ventas.

Aprende más sobre el programa de seguridad de productos de Lenovo.



¹ ITC: "2022 Global Server Hardware Security Survey", Septiembre 2022.

² Blue Voyant: "The State of Supply Chain Defense: Annual Global Insights Report 2022".

³ Security Magazine: "98% das organizações foram impactadas por uma violação de segurança na cadeia de suprimentos", Noviembre 2022.

⁴ Microsoft: "New Security Signals study shows firmware attacks on the rise; here's how Microsoft is working to help eliminate this entire class of threats", Marzo 2021.

⁵ McKinsey & Company: "Taking the pulse of shifting supply chains", Agosto 2022. Os dados citados são referenciados de "McKinsey global survey of supply chain leaders Mar-Apr 2022".

⁶ Security Info Watch: "The cybersecurity implications of quantum computing", Febrero 2023.

⁷ Verizon: "DBIR: Data Breach Investigations Report", 2022.

⁸ VirusTotal: "Ransomware in a Global Context", Octubre 2021.