¿Quieres prepararte ante un ciberataque? 4 consejos para un plan de recuperación de datos

Las amenazas al ecosistema de TI son inevitables, desde ciberataques, hasta emergencias climáticas como incendios forestales y huracanes hasta errores del equipo de TI. Si bien, no se puede controlar todas las variables que pueden ocurrir, es recomendable enfocarse en aumentar la resiliencia empresarial con un plan robusto de recuperación de datos.

Como afirma el analista Gartner, "intentar improvisar un proceso de recuperación después de un ataque conducirá inevitablemente a errores y prolongará la interrupción".

Pero, ¿qué incluye un plan de recuperación de datos? ¿Cómo asegurarse de que será efectivo? Es necesario agruparlo en cuatro áreas clave:

- **Inventario de datos y aplicaciones:** El primer paso es agrupar datos. ¿Qué datos y aplicaciones son más esenciales para la organización? ¿Sin qué elementos se puede sobrevivir? ¿Qué datos son en su mayoría estáticos? ¿Exactamente dónde se encuentran los datos? Para decidir qué datos entran en cada categoría, es necesario pensar qué tan vitales son para el negocio. Por ejemplo, herramientas como Microsoft 365 y SharePoint son esenciales para la colaboración y la comunicación, por lo que los datos confidenciales almacenados allí pueden asignarse a una clasificación más alta.
  La clasificación más alta, de misión crítica, incluye las bases de datos utilizadas para transacciones financieras. Active Directory también entra directamente en esta categoría, ya que proporciona los servicios de autenticación y autorización que permiten que el ecosistema de TI funcione. Sin Active Directory, los usuarios no pueden iniciar sesión en sus dispositivos, ni acceder a las aplicaciones y los servicios. "El proceso de restauración de muchos ataques de ransomware bien documentados se ha visto obstaculizado por no tener un proceso de restauración de Active Directory intacto", dice Gartner.

- **Establecer objetivos:** A continuación, es momento de establecer el objetivo de tiempo de recuperación (RTO) y el objetivo de punto de recuperación (RPO) para cada tipo de datos. Se debe trabajar con las partes interesadas para determinar qué tan rápido se deben restaurar los datos y qué cantidad de pérdida es aceptable.
- **Descubrir y evaluar vulnerabilidades**: Otro paso es descubrir las debilidades que los hackers pueden aprovechar y luego priorizarlas evaluando tanto la probabilidad de que eso suceda como el daño potencial que podría resultar.
  Durante este proceso, hay que considerar tanto las amenazas internas como los ataques externos. Los piratas informáticos ahora intentan activamente sobornar a los empleados para implementar malware, por ejemplo. Es vital trabajar para establecer un modelo Zero Trust.

- **Tener más de una copia de seguridad de los datos:** Todo plan de recuperación de

datos debe cubrir las ubicaciones y los formatos de las copias de seguridad. La estrategia clásica es 3-2-1: tener tres copias en dos medios de almacenamiento diferentes con una copia fuera del sitio. También es fundamental analizar detenidamente al proveedor de los servicios en la nube y los detalles del acuerdo con ellos para tener la seguridad de que éste puede cumplir con los objetivos de recuperación.

- **Automatizar:** Los procesos manuales son inherentemente lentos, poco confiables y propensos a errores humanos. Por ello, la automatización es quizás aún más vital para las operaciones de recuperación, especialmente la recuperación ante desastres, cuando cada segundo de tiempo de inactividad le cuesta a la empresa. Como dice Gartner, "La pronta recuperación de los sistemas afectados será imposible si las organizaciones tienen que depender de procesos y procedimientos manuales".

Ninguna organización es inmune a las ciberamenazas modernas; afectan a todos, desde las PYMES hasta las grandes empresas, o dependencias de gobierno. También son vulnerables a los desastres naturales, las amenazas internas, los errores y otros riesgos.

La pregunta es, ¿qué tan rápido y qué tan bien puede una empresa recuperarse cuando ocurre un desastre? Para lograr la resiliencia cibernética necesaria para proteger una organización, se debe crear un plan sólido de recuperación de datos y probarlo con regularidad.