¿Por qué la copia de seguridad y recuperación no es suficiente para hacer frente al ransomware?

Respuesta breve: Las copias de seguridad abordan solo la etapa final de un ataque de ransomware: el cifrado. Para cuando comienza el cifrado, los atacantes generalmente ya han robado credenciales y extraído sus datos. Restaurar desde una copia de seguridad recupera sus archivos; no hace nada respecto a los datos que ya están en manos del atacante.

El ransomware es el último paso, no el primero

Una intrusión típica se desarrolla en tres etapas:

1. **Robo de identidad** — se comprometen credenciales para obtener acceso.
2. **Robo de datos** — se exfiltran propiedad intelectual, registros de clientes y otros datos sensibles.
3. **Cifrado** — los archivos se bloquean y se exige un rescate.

Las estrategias de recuperación entran en juego solo en la tercera etapa. La violación de confidencialidad y la pérdida de control operativo ya han ocurrido.

El costo real

El mayor riesgo empresarial del ransomware generalmente no es el rescate en sí, sino los ingresos perdidos por una interrupción prolongada y el daño reputacional que le sigue. Prevenir el compromiso inicial protege ambos aspectos, razón por la cual la prevención debe preceder a la planificación de recuperación, en lugar de reemplazarla.

Revision #1
Created 2026-07-24 01:46:40 UTC by Dennis Underwood
Updated 2026-07-24 01:46:40 UTC by Dennis Underwood