

Por que backup e recuperação não são suficientes para lidar com ransomware?

Resposta curta: Os backups tratam apenas do estágio final de um ataque de ransomware — a criptografia. Quando a criptografia começa, os atacantes já costumam ter roubado credenciais e exfiltrado seus dados. Restaurar a partir do backup recupera seus arquivos; isso não faz nada em relação aos dados que já estão nas mãos do atacante.

O ransomware é a última etapa, não a primeira

Uma intrusão típica ocorre em três estágios:

1. **Roubo de identidade** — credenciais são comprometidas para obter acesso.
2. **Roubo de dados** — propriedade intelectual, registros de clientes e outros dados sensíveis são exfiltrados.
3. **Criptografia** — arquivos são bloqueados e um resgate é exigido.

As estratégias de recuperação atuam somente no terceiro estágio. A violação de confidencialidade e a perda de controle operacional já ocorreram.

O custo real

O maior risco de negócio decorrente do ransomware geralmente não é o resgate em si — é a receita perdida devido a uma interrupção prolongada e os danos à reputação que se seguem. Prevenir o comprometimento inicial protege ambos, motivo pelo qual a prevenção deve vir antes do planejamento de recuperação, e não em seu lugar.

Revision #1

Created 2026-07-24 05:44:50 UTC by Dennis Underwood

Updated 2026-07-24 05:44:50 UTC by Dennis Underwood