¿Debería la ciberseguridad centrarse en la resiliencia o en prevenir los ataques desde el principio?

Respuesta breve: La resiliencia —recuperarse después de un ataque— es importante, pero el objetivo más importante es prevenir el ransomware, el robo de datos y el robo de identidad antes de que se produzca el daño, ya que los ataques automatizados son incesantes y cada vez están mejor informados sobre cuándo atacar.

Dos significados de "resiliencia"

El término "resiliencia" en ciberseguridad ha derivado hacia dos ideas distintas. Una es si las propias herramientas de seguridad pueden seguir funcionando bajo ataque —esencialmente, si el software destinado a protegerlo puede sobrevivir a ser atacado o manipulado directamente, de manera similar a preguntarse si una cámara de seguridad puede seguir grabando después de que alguien intente desactivarla. La otra, de significado más tradicional, es si su negocio puede recuperarse y salir adelante después de que ya se haya producido una brecha.

Ambas son importantes, pero ninguna debería ser la estrategia principal. Los ataques modernos son automatizados y constantes. La razón principal por la que las organizaciones no son atacadas sin cesar es que los atacantes se han vuelto expertos en leer señales sobre qué objetivos merecen su tiempo —por ejemplo, evitando a empresas que claramente no cuentan con los recursos financieros para hacer rentable un ataque. Ese nivel de selección automatizada de objetivos significa que la resiliencia por sí sola es una postura reactiva frente a un adversario que siempre está sondeando.

Por qué la prevención debe ser lo primero

Ser resiliente después de una brecha es comparable a tener un buen taller de reparación de confianza después de un accidente automovilístico. Es útil, pero es mucho mejor evitar el accidente por completo. Nadie quiere poner a prueba lo bien que funciona el proceso de reparación si, en

cambio, puede evitar la colisión desde el principio.

Aplicado a la seguridad empresarial, esto significa que la prioridad debe ser detener los ataques antes de que tengan éxito —el equivalente a tener frenos confiables en lugar de solo un buen plan de reparación para después de un choque. Cyber Crucible avanza hacia este resultado centrándose en la prevención autónoma, con el objetivo de detener los intentos de ransomware, robo de datos y robo de identidad antes de que puedan causar daño, en lugar de depender únicamente de la recuperación y la limpieza posteriores.

https://player.vimeo.com/video/1194994916

Ver en Vimeo · Subtítulos: English, Français, Español, العربية

Revision #1
Created 2026-07-24 02:12:01 UTC by Dennis Underwood
Updated 2026-07-24 02:12:01 UTC by Dennis Underwood