A segurança cibernética deve focar-se na resiliência ou na prevenção de ataques antes que ocorram?

Resposta rápida: A resiliência—recuperar-se após um ataque—é importante, mas o objetivo mais relevante é prevenir ransomware, roubo de dados e roubo de identidade antes que o dano ocorra, uma vez que os ataques automatizados são incessantes e cada vez mais bem informados sobre o momento certo para atacar.

Dois Significados de "Resiliência"

O termo "resiliência" em segurança cibernética tem-se desviado para duas ideias diferentes. Uma é se as próprias ferramentas de segurança conseguem continuar a funcionar sob ataque—essencialmente, se o software destinado a proteger consegue sobreviver a ser diretamente alvo ou adulterado, de forma semelhante a perguntar se uma câmara de segurança consegue continuar a gravar depois de alguém tentar desativá-la. O outro significado, mais tradicional, é se a empresa consegue recuperar e retomar a normalidade depois de uma violação já ter ocorrido.

Ambos são importantes, mas nenhum deles deve ser a estratégia principal. Os ataques modernos são automatizados e constantes. A principal razão pela qual as organizações não são atacadas continuamente é que os atacantes se tornaram hábeis em interpretar sinais sobre quais são os alvos que valem o seu tempo—por exemplo, evitando empresas que claramente não têm os recursos financeiros que tornem um ataque rentável. Este nível de segmentação automatizada significa que a resiliência, por si só, é uma postura reativa contra um adversário que está sempre a sondar.

Por Que a Prevenção Deve Vir Primeiro

Ser resiliente após uma violação é comparável a ter uma boa oficina de reparação de automóveis já identificada depois de um acidente de carro. É útil, mas é muito melhor evitar completamente o acidente. Ninguém quer testar o quão bem funciona o processo de reparação se puder, em vez disso, evitar a colisão em primeiro lugar.

Aplicado à segurança empresarial, isto significa que a prioridade deve ser impedir os ataques antes que sejam bem-sucedidos—o equivalente a ter travões fiáveis em vez de apenas um bom plano de reparação para depois de um acidente. A Cyber Crucible trabalha nesse sentido, concentrando-se na prevenção autónoma, com o objetivo de deter tentativas de ransomware, roubo de dados e roubo de identidade antes que possam causar danos, em vez de depender apenas da recuperação e da limpeza após o facto.

https://player.vimeo.com/video/1194994916?texttrack=pt

Ver no Vimeo · Legendas: English, Français, Español, العربية

Revision #2
Created 2026-07-24 06:10:47 UTC by Dennis Underwood
Updated 2026-08-06 18:37:37 UTC by Dennis Underwood