La cybersécurité doit-elle se concentrer sur la résilience ou sur la prévention des attaques dès le départ ?

Réponse courte : La résilience — se rétablir après une attaque — a de l'importance, mais l'objectif le plus important est de prévenir les rançongiciels, le vol de données et l'usurpation d'identité avant que des dommages ne surviennent, car les attaques automatisées sont incessantes et de plus en plus bien informées sur le moment opportun pour frapper.

Deux significations de la « résilience »

Le terme « résilience » en cybersécurité a évolué vers deux idées différentes. La première est de savoir si vos outils de sécurité eux-mêmes peuvent continuer à fonctionner sous une attaque — c'est-à-dire si le logiciel censé vous protéger peut survivre à une attaque ou à une tentative de sabotage directe, un peu comme se demander si une caméra de sécurité peut continuer à enregistrer après qu'on ait tenté de la désactiver. L'autre signification, plus traditionnelle, est de savoir si votre entreprise peut se rétablir et rebondir après qu'une violation s'est déjà produite.

Les deux comptent, mais aucune ne devrait constituer la stratégie principale. Les attaques modernes sont automatisées et constantes. La principale raison pour laquelle les organisations ne sont pas frappées sans relâche est que les attaquants sont devenus experts dans la lecture des signaux indiquant quelles cibles valent la peine d'être visées — par exemple, en évitant les entreprises qui n'ont manifestement pas les ressources financières permettant de rendre une attaque rentable. Ce niveau de ciblage automatisé signifie que la résilience seule constitue une posture réactive face à un adversaire qui sonde en permanence.

Pourquoi la prévention doit venir en premier

Être résilient après une violation est comparable au fait d'avoir un bon garage de réparation à disposition après un accident de voiture. C'est utile, mais il est bien préférable d'éviter complètement l'accident. Personne ne veut tester l'efficacité du processus de réparation s'il peut

plutôt éviter la collision dès le départ.

Appliqué à la sécurité des entreprises, cela signifie que la priorité doit être d'arrêter les attaques avant qu'elles ne réussissent — l'équivalent d'avoir des freins fiables plutôt qu'un simple bon plan de réparation après un accident. Cyber Crucible œuvre en ce sens en se concentrant sur la prévention autonome, avec pour objectif d'arrêter les tentatives de rançongiciel, de vol de données et d'usurpation d'identité avant qu'elles ne puissent causer des dommages, plutôt que de dépendre uniquement du rétablissement et du nettoyage après coup.

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

Regarder sur Vimeo · Sous-titres : English, Français, Español, العربية

Revision #1
Created 2026-07-24 07:23:02 UTC by Dennis Underwood
Updated 2026-07-24 07:23:02 UTC by Dennis Underwood