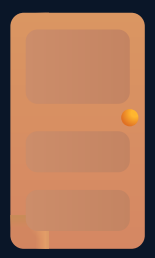

Il rentre par la porte la moins surveillée

Phase 2 sur 4. Pas par la grande porte. Par la porte oubliée.

Intrusion

Un seul point d'entrée suffit. La phase la plus rentable pour l'attaquant — où la plupart des PME perdent.

Dans 9 attaques sur 10

Phishing personnalisé

Email qui parle d'un vrai dossier. Données issues de la phase R.

MDP faible / réutilisé

Le mot de passe LinkedIn de 2019 qui ouvre M365 aujourd'hui.

RDP / VPN exposé

Service oublié, firmware obsolète, vulnérabilité publique.

Vulnérabilité non patchée

Windows Server jamais MAJ, Exchange laissé sur place.

1 point d'entrée suffit

La phase I est la plus rentable pour le hacker — et celle où la plupart des PME perdent par manque d'inventaire.

> « On savait pas que ce serveur était exposé. » — La phrase entendue après 80% des intrusions PME.

4 contre-mesures

Chacune ferme une voie d'entrée. Ensemble, elles bloquent 90% des intrusions PME.

MFA partout

Couvre les voies 1, 2 et 3 simultanément. Le levier le plus rentable.

EDR centralisé

Intercepte les exécutions suspectes même après une compromission.

Fermeture services exposés

Pas de RDP direct. VPN avec MFA. Audit trimestriel des ports.

Cycle de patch mensuel

Sans exception, même sur serveurs « critiques ».

R.I.P. en 4 phases

Une attaque cyber suit un parcours prévisible. À chaque étape, il existe un moyen de la couper.

R

Reconnaissance

Limiter expo · monitoring leaks

I

Intrusion

Vous êtes ici

P

Propagation

EDR centralisé · segmentation

†

Impact

Sauvegardes testées · plan crise

La semaine prochaine
Phase 3 — Propagation

Une fois rentré, le hacker rebondit. Phase la plus longue. Phase la plus visible **si on sait regarder**.

Et concrètement chez vous ?

Diagnostic 2h sur place sans engagement

Tél +41 78 811 92 21

Email eric.darien@abaxinfo.com

Web diagnostic.abaxinfo.com