# Branché ne veut pas dire protégé

En 3 minutes, un collaborateur peut ouvrir une porte que votre pare-feu ne voit même pas.

# Presque jamais de la malveillance

Quelqu'un veut accéder à son poste depuis la maison. Il installe un outil de tunnel qui marche tout de suite.

Le trafic passe **à côté du pare-feu** et de la surveillance. Sans bruit.

# Le Shadow IT

Des outils installés dans votre dos, souvent avec les meilleures intentions du monde.

> **Résultat : des angles morts que personne ne contrôle, et une porte d'entrée de plus.**

# Un boîtier qui rassure

Un pare-feu acheté puis laissé sur ses **réglages d'usine**, c'est un boîtier rassurant qui ne fait pas son travail.

Vous vous croyez protégé. Vous ne l'êtes pas.

# 5 gestes qui changent tout

1. **Filtrer ce qui sort**
   Pas seulement ce qui entre.

2. **Bloquer les tunnels et VPN grand public**
   Par catégorie, au pare-feu et au DNS.

3. **Contrôler les installations**
   Ce qui peut s'installer sur les postes.

4. **Segmenter le réseau**
   Une personne n'atteint jamais tout le réseau.

5. **Superviser les alertes**
   Garder un oeil, en continu.

# La règle qu'on s'applique

Le jour où nous déployons ce type d'outil chez un client, nous posons ces protections en même temps.

Sinon, nous créerions nous-mêmes la faille que nous sommes censés refermer.

# À se poser aujourd'hui

- 🧩 Qui peut installer un logiciel sur les postes ?
- 📤 Sait-on vraiment ce qui sort du réseau ?
- 🚧 Le pare-feu bloque-t-il les VPN grand public ?

Votre pare-feu, paramétré ou juste branché ?

# Une revue courte de ce qui sort

Tél +41 78 811 92 21

Email eric.darien@abaxinfo.com

Web abaxinfo.com