Le « facteur humain », plafond de verre de l'authentification forte ?

Dans quelle mesure le « facteur humain » dicte-t-il le choix des solutions d'authentification multifacteur ? On peut se poser la question au regard du commentaire qu'un membre de la Microsoft Tech Community a publié en réaction à un post d'Alex Weinert.

Ce dernier dirige l'équipe Identity Security au sein du groupe américain. Dans sa démarche d'évangélisation, il avait d'abord axé sa communication sur la faiblesse des mots de passe. Avant de commencer à hiérarchiser les méthodes d'authentification forte. Jusqu'à en appeler, cette semaine, à abandonner les SMS et les appels vocaux.

Son principal argument : la fragilité du canal de transport des informations. En l'occurrence, le réseau 2G, dont on reconnaît aujourd'hui les limites en matière de chiffrement. Autre écueil : l'implication d'opérateurs télécoms. Lesquels peuvent eux-mêmes représenter un point faible, en plus d'introduire de l'opacité pour les fournisseurs de services d'authentification multifacteur.

Réfléchir avant d'agir

De manière générale, explique Alex Weinert, plus les textos s'implantent dans les stratégies d'authentification forte, plus l'intérêt des pirates informatiques grandit. Les outils *open source* à leur disposition ne manquent pas, tout comme les services (*femtocells*, SS7, radios logicielles…).

« *Pour la plupart des utilisateurs, nous pensons que la bonne réponse réside dans les applications d'authentification* », résume Alex Weinert. Ces dernières, en plus de reposer sur des réseaux réputés plus sécurisés, offrent un potentiel de contextualisation des accès.
L'intéressé ne nie pas qu'il existe des méthodes encore plus sûres. Aussi bien face aux risques de prise de contrôle du canal de communication que de *phishing* en temps réel. En particulier, les clés de sécurité physiques. Même si de nombreuses applications restent incompatibles.

Alors le SMS, bon à jeter aux orties ? Pas pour l'auteur du commentaire sus-évoqué. « *Ce qui me fait peur avec* [les applications d'authentification]*, c'est que beaucoup de mes utilisateurs ne sont pas attentifs*, explique-t-il. *Ils approuveraient toute demande. Bien trop semblent prédisposés à cliquer sur « Oui » ou sur « Autoriser » sans comprendre (ou sans même se donner la peine de lire) ce sur quoi ils cliquent*. *Au moins, avec les SMS, les tentatives frauduleuses de connexion ne remontent pas jusqu'à l'attaquant* », conclut-il.

Photo d'illustration © twobee – Fotolia