Zoom active la double authentification en natif

Pas de traitement différencié cette fois-ci* : tous les utilisateurs de Zoom ont droit à la double authentification.

L'entreprise américaine vient d'officialiser l'activation globale de cette fonctionnalité.
La version web et le client mobile ne la prennent pas encore en charge. Il est nécessaire d'utiliser l'application de bureau (version 5.2.2 et ultérieures) ou la solution Zoom Rooms (5.2.1 et plus) pour les salles de conférence.

Peuvent faire office de deuxième facteur :

- appel ;
- SMS ;
- application mobile fondée sur l'algorithme TOTP (Zoom recommande Google Authenticator, Microsoft Authenticator et FreeOTP).

La double authentification native à Zoom s'active dans les paramètres avancés de sécurité, avec un profil d'admin ou de titulaire du compte. On peut la définir pour :

- Tous les utilisateurs rattachés à un compte
- Des rôles spécifiques (titulaire, administrateur, membre)
- Des groupes spécifiques

On rappellera que les comptes payants (Pro, Affaires, Éducation, Entreprise) disposent d'autres options « avancées ». Notamment, sur les mots de passe :

- Imposer une longueur minimale (de 8 à 14 caractères)
- Obliger l'emploi d'au moins un caractère spécial
- Planifier l'expiration automatique (après 30, 60, 90 ou 120 jours)
- Empêcher la réutilisation d'un mot de passe précédemment défini (les 3 à 12 dernières fois)
- Limiter le nombre de changements par période de 24 h (3 à 8 fois)

** Zoom n'avait pas eu la même logique sur le chiffrement de bout en bout. En tout cas initialement : il était*

prévu de le réserver aux comptes payants. Sous les critiques, l'éditeur avait fini par faire volte-face.

Photo d'illustration via *shutterstock.com*