Authentification multifacteur (MFA)

L'authentification multifacteur vous aide à vous défendre contre les cybercriminels

De nombreuses cyber-attaques nécessitent l'accès au réseau ou aux emails de l'entreprise. Quand ces accès sont simplement protégés par un identifiant utilisateur et un mot de passe (authentification à un seul facteur, SFA), les cybercriminels parviennent aisément à accéder au système informatique de l'entreprise.

Dès qu'un hacker a accès à vos e-mails, il peut utiliser votre identité pour envoyer de faux e-mails ou, s'il a accès à votre réseau, espionner votre environnement, augmenter ses privilèges, supprimer des sauvegardes et déployer des rançongiciels.

Pour ce faire, les hackers peuvent utiliser plusieurs méthodes :

- **Attaque par force brute** ou utilisation d'un outil qui permet de pirater les mots de passe en essayant de manière automatisée une grande quantité de mots de passe courants.
- **Récupération de données d'identification** ou profiter du fait que de nombreuses personnes utilisent souvent les mêmes combinaisons d'identifiants et de mots de passe pour leurs différents comptes.
- **Hameçonnage** ou envoi par e-mail d'une fausse demande de réinitialisation du mot de passe, qui permet de récupérer les informations nécessaires à l'accès aux e-mails professionnels du collaborateur concerné.

Une des méthodes les plus efficaces pour empêcher les cybercriminels d'accéder à vos systèmes est probablement l'authentification multifacteur (MFA) car elle offre un deuxième niveau d'authentification/de protection.

Qu'est-ce que la MFA ?

La MFA exige au moins deux facteurs d'authentification ou preuves d'identité pour s'assurer que les personnes qui souhaitent accéder aux e-mails de l'entreprise ou à d'autres éléments importants, sont bien celles qu'elles prétendent être.

Exemple d'une authentification à trois niveaux :

1. 

Quelque chose que vous connaissez
(généralement un mot de passe ou un code de vérification)

2. 

Quelque chose que vous possédez
(un appareil de confiance qui ne peut être dupliqué facilement, tel qu'un téléphone ou une clé de sécurité par exemple)

3. 

Quelque chose que vous êtes
(biométrie)

> ***Il n'est pas simple pour les criminels de compromettre deux facteurs d'authentification ou plus : le risque d'une compromission est ainsi considérablement réduit.***

Pourquoi la MFA est-elle si importante ?

Le concept de l'authentification multifacteur repose sur la moindre probabilité qu'un hacker soit en mesure de détenir à la fois quelque chose que connait et quelque chose que possède l'utilisateur. Dans le cas d'un compte de messagerie, son utilisateur possède le jeton logiciel (soft token) correspondant ou l'appareil avec lequel un code unique et de courte durée peut être généré.

Activer la MFA

Une authentification multifacteur peut être une des mesures les plus rapides et les plus efficaces pour protéger l'identité des utilisateurs. De nombreux services web, voire la majorité d'entre eux, disposent d'une option MFA, bien qu'elle soit souvent désactivée par défaut.

Demandez conseil à des experts pour savoir comment activer la MFA la mieux adaptée à votre entreprise.

Chubb. Insured.℠