Authentification multifacteur (MFA)

Les cyber-attaques impliquent dans de nombreux cas que les hackers aient accès au réseau ou aux e-mails d'une entreprise. Avec un accès courant par identifiant utilisateur et mot de passe (appelé aussi authentification à un seul facteur, SFA), les cybercriminels peuvent sans trop de difficultés accéder au système informatique d'une entreprise.

La MFA vous aide à vous défendre contre les cybercriminels

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

Pour ce faire, les hackers peuvent utiliser plusieurs méthodes :

- **Utilisation de la force brutale** ou d'un outil qui permet de pirater les mots de passe en essayant de manière automatisée une grande quantité de mots de passe courants.
- **Interception des 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 d'intercepter les données figurant dans les 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 votre entreprise ou à d'autres éléments importants de votre entreprise, sont aussi celles qu'elles prétendent être.

Exemple d'une authentification à trois niveaux:

1. 

Une information que vous connaissez
((normalement un mot de passe ou un code de vérification)

2. 

Un objet en votre possession
(un appareil de confiance qui ne peut pas être dupliqué facilement, par exemple un téléphone ou une clé de sécurité)

3. 

Une caractéristique personnelle
(biométrie)

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

Pourquoi la MFA est-elle si importante?

Le concept de l'authentification à plusieurs niveaux repose sur le fait que les cybercriminels peuvent certes voler ce que les utilisateurs légitimes connaissent, mais il est beaucoup plus improbable qu'ils possèdent aussi l'objet ou la caractéristique personnelle de ces utilisateurs. 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.

Implémenter la MFA

Une authentification à plusieurs niveaux 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 qui est cependant souvent désactivée par défaut.

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

Chubb. Insured.℠

Chubb Versicherungen (Schweiz) AG / Chubb Insurance (Switzerland) Limited / Chubb Assurances (Suisse) SA. Bärengasse 32, 8001 Zürich, T + 41 43 456 76 00, www.chubb.com/ch-fr

CH-FRO426-MD 06/22