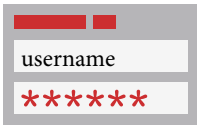
TRAVELERS

Authentification à facteurs multiples

Qu'est-ce que l'authentification à facteurs multiples?

L'authentification à facteurs multiples est l'utilisation d'au moins deux facteurs d'authentification différents. L'authentification à facteurs multiples est validée lorsqu'au moins deux de ces catégories d'identification sont requises pour vérifier avec succès l'identité d'un utilisateur ***avant*** de lui accorder l'accès.



1. QUELQUE CHOSE QUE VOUS SAVEZ

Un mot de passe ou une phrase de passe est quelque chose que vous connaissez.

2. QUELQUE CHOSE QUE VOUS POSSÉDEZ

Un jeton ou une carte à puce est quelque chose que vous possédez.

3. QUELQUE CHOSE QUE VOUS ÊTES

L'identification biométrique par le biais d'une empreinte digitale ou d'un balayage de la rétine établit qui vous êtes.

Il existe une certaine souplesse quant aux authentifications utilisées par une entreprise pour valider l'identité d'un utilisateur sans inconvénient excessif.

Pourquoi l'authentification à facteurs multiples est-elle essentielle?

99,9%

des attaques de compromission de comptes peuvent être bloquées par l'authentification à facteurs multiples[1]

94%

des victimes d'attaques de rançongiciels qui ont fait l'objet d'une enquête n'utilisaient pas d'authentification à facteurs multiples[2]

L'authentification à facteurs multiples contribue à protéger une entreprise en ajoutant une mesure de sécurité supplémentaire, ce qui rend l'accès aux systèmes de l'entreprise plus difficile pour les cybercriminels. Les informations d'identification telles que les identifiants et les mots de passe peuvent constituer le maillon faible de la cybersécurité d'une entreprise, car elles sont souvent compromises et publiées sur le Web caché. Et les mots de passe sont de moins en moins sûrs. À mesure que les utilisateurs se connectent à des systèmes nécessitant un identifiant et un mot de passe, ils ont tendance à devenir paresseux. Ils créent des mots de passe simples et faciles à deviner, utilisent le même mot de passe pour différents sites, les partagent et les donnent parfois par inadvertance à un pirate informatique.

Que devrions-nous protéger à l'aide d'une authentification à facteurs multiples?

Accès réseau à distance

L'authentification à facteurs multiples pour l'accès réseau à distance est un contrôle de sécurité important qui peut aider à réduire le potentiel de compromission du réseau causé par des mots de passe perdus ou volés. Sans ce contrôle, un intrus peut accéder à un réseau d'entreprise de la même manière qu'un utilisateur autorisé.

Accès privilégié/administratif

L'authentification à facteurs multiples pour l'accès à distance et interne aux comptes administratifs permet d'empêcher les intrus qui ont compromis un système interne de renforcer leurs privilèges et d'obtenir un accès plus large à un réseau compromis. Cela peut empêcher un pirate d'obtenir le niveau d'accès nécessaire pour déployer avec succès un rançongiciel sur le réseau, effacer les journaux d'activité, créer de faux comptes d'utilisateur ou même désactiver un anti-programme malveillant.

Accès à distance au courrier électronique

Lors de l'accès à la messagerie électronique par le biais d'un site Web ou d'un service en nuage sur des appareils non professionnels, l'authentification à facteurs multiples peut contribuer à réduire la capacité d'un intrus à accéder au compte de messagerie professionnelle d'un utilisateur. Les auteurs de menaces utilisent souvent l'accès au courrier électronique pour perpétrer divers stratagèmes de cybercriminalité contre les entreprises et leurs clients.

[1] Source: https://www.microsoft.com/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/

[2] Source: Arete Presentation "Ransomware Cards" 7-31-2020

Pour en savoir plus, parlez à votre courtier ou visitez travelerscanada.ca/fr/cyberrisques.

TRAVELERS

travelerscanada.ca