Cyberconseils : Authentification multifactorielle

VICTOR

L'authentification multifactorielle exige des facteurs de vérification supplémentaires pour s'assurer qu'un utilisateur est bien celui qu'il prétend être. Les conseils ci-dessous expliquent pourquoi l'authentification multifactorielle est essentielle pour la sécurité dans le contexte actuel de menaces, les éléments à prendre en compte pour la mettre en œuvre et les ressources supplémentaires pour l'aider à la mettre en place.

Qu'est-ce que l'authentification multifactorielle?

L'authentification multifactorielle est un mécanisme de sécurité qui exige deux méthodes d'authentification ou plus afin de vérifier l'identité d'un utilisateur qui tente d'accéder à une ressource informatique, par exemple, un compte de courriel ou un compte administrateur sur un serveur. L'authentification multifactorielle combine deux facteurs ou plus : quelque chose que l'utilisateur connaît (par exemple, un mot de passe ou une phrase de passe), quelque chose que l'utilisateur possède (un jeton de sécurité) et ce que l'utilisateur est (une vérification biométrique, par exemple, une empreinte digitale ou une reconnaissance faciale).

Pourquoi est-ce important?

L'authentification multifactorielle est extrêmement importante en raison de la sophistication croissante des cyberattaques. L'authentification multifactorielle peut empêcher les cybercriminels malveillants d'accéder à vos données ou à celles de votre entreprise. Même si votre mot de passe est entre les mains d'un cybercriminel, il est peu probable qu'il dispose également de vos autres moyens de vérification.

Même si votre mot de passe est entre les mains d'un cybercriminel, il est peu probable qu'il dispose également de vos autres moyens de vérification. C'est ce qui rend l'authentification multifactorielle si importante.

Quand dois-je utiliser l'authentification multifactorielle?

- Entreprises – Dans la mesure du possible, la fonctionnalité d'authentification multifactorielle doit toujours être activée pour tous les membres du personnel lorsqu'ils utilisent des logiciels liés au serveur, des applications accessibles de l'extérieur, par exemple, Microsoft Office 365 ou Google Workspace ou d'autres applications similaires.
- Particuliers – Dans la mesure du possible, il est conseillé aux particuliers d'activer l'authentification multifactorielle lorsqu'ils accèdent à des sites Web qui nécessitent la soumission ou l'accès à des renseignements financiers, lorsqu'ils soumettent des renseignements personnels sensibles ou lorsqu'ils accèdent à des comptes de courriel.

Où puis-je l'utiliser?

Vous pouvez utiliser l'authentification multifactorielle avec tout site Web ou toute application qui a activé cette fonctionnalité. Microsoft a activé la fonction d'authentification multifactorielle pour ses applications et ses sites Web, tout comme Google et d'autres entreprises de technologie.

Comment puis-je la mettre en place?

L'authentification multifactorielle peut être mise en place de plusieurs façons, selon le type de jeton de sécurité ou autre facteur de vérification choisi pour l'authentification. Cependant, la mise en œuvre de l'authentification multifactorielle nécessite une réflexion et une planification minutieuses, en particulier pour les grandes organisations.

Les facteurs à prendre en compte sont :

- Être conscient de ce que vous voulez protéger
- Comprendre la technologie d'authentification multifactorielle que vous allez utiliser
- Comprendre l'impact sur les employés et les sensibiliser à l'authentification multifactorielle

Lors du déploiement de l'authentification multifactorielle, il est conseillé de commencer par vos comptes les plus importants, par exemple, les comptes administrateurs. Ce sont les cibles de grande valeur que les cybercriminels souhaitent viser, car ils peuvent utiliser ces comptes pour passer à travers l'organisation. Ensuite, déployez l'authentification multifactorielle pour les utilisateurs privilégiés ayant des rôles commerciaux clés ou pour ceux qui ont accès à des communications commerciales importantes ou sensibles.

La réalisation de ce qui suit contribuera à la réussite du déploiement de l'authentification multifactorielle :

- Faire l'inventaire des systèmes et des applications. Savoir ce que vous avez permettra de déterminer les systèmes prioritaires.
- Classer les systèmes par ordre de priorité en fonction de la criticité et de la sensibilité des données auxquelles vous accédez.
- Mettre en place un processus d'accueil pour le personnel et pour les applications logicielles.
- Tester le fonctionnement des applications avec l'authentification multifactorielle avant le déploiement.

Visitez assurancevictor.ca/cyber.

Renseignements supplémentaires

- Gouvernement du Canada – Centre canadien pour la cybersécurité
  - › Sécurisez vos comptes et vos appareils avec une authentification multifactorielle
- Une ressource d'apprentissage sur l'authentification multifactorielle pour les entreprises utilisant Microsoft peut être trouvée ici.
- Pour un tutoriel sur la façon d'activer l'authentification multifactorielle dans Microsoft Azure, cliquez ici.
- Les instructions sur la façon de configurer l'authentification multifactorielle dans Microsoft Office 365 peuvent être trouvées ici.
- Une trousse de déploiement de l'authentification multifactorielle contenant des affiches personnalisables et des modèles de courriel pour les entreprises est disponible ici (en anglais uniquement).
- Un guide de configuration de l'authentification multifactorielle pour Google Workspace est ici.
- Ressources cybernétiques de Victor
  - › Assurance contre les cyber-risques de Victor
  - › Guide : Risques liés à la cyber-responsabilité : Comment vous protéger, ainsi que votre entreprise
  - › Guide : Cybersécurité : Travailler en toute sécurité depuis son domicile
  - › Infographie : Les cyberattaques : Une menace pour toutes les entreprises
  - › Vidéo : Une journée dans la vie d'un propriétaire d'entreprise dans un cybermonde
  - › Vidéo : Les experts de Victor partagent les mesures préventives alors que les cyberattaques se multiplient

#LaMenaceEstRéelle