SÉCURISEZ VOS COMPTES ET VOS APPAREILS AVEC UNE AUTHENTIFICATION MULTIFACTEUR

juin 2020

ITSAP.30.030

Tant les organisations que les personnes peuvent tirer avantage de l'authentification multifacteur pour ce qui est de sécuriser leurs dispositifs et leurs comptes. Si ce mode d'authentification est activé, il faudra utiliser deux facteurs d'authentification distincts ou plus pour déverrouiller un dispositif ou se connecter à un compte. Que ce soit pour l'accès aux courriels, au stockage en nuage ou aux services bancaires en ligne, l'authentification multifacteur fournit également une couche de sécurité supplémentaire contre les cyberattaques comme le bourrage d'identifiants. Dans le cas d'une attaque par bourrage d'identifiants, les pirates informatiques utilisent des justificatifs d'identités d'un site en particulier précédemment volés en espérant que vous les ayez utilisés pour d'autres comptes. propose une couche de protection supplémentaire. Si ce n'est pas déjà le cas, il est fortement recommandé à votre organisation et vous d'avoir recours à l'authentification multifacteur, dans la mesure du possible, pour protéger vos données et vos services opérationnels à valeur élevée contre les auteurs de menace.

QUELS SONT LES FACTEURS D'AUTHENTIFICATION?

L'authentification multifacteur emploie une combinaison des facteurs suivants pour authentifier un utilisateur :

- **Quelque chose que vous connaissez :** Il s'agit généralement de votre phrase de passe, de votre mot de passe ou de votre NIP. Comme il est facile de compromettre ce facteur, il est fortement recommandé d'en ajouter un autre si cela s'avère possible;
- **Quelque chose que vous avez :** Il peut s'agir d'un jeton matériel, comme une clé USB ou une carte d'accès, ou encore d'un jeton logiciel, comme un logiciel d'authentification;
- **Quelque chose qui vous caractérise :** Ce facteur repose sur une caractéristique biométrique unique comme la lecture rétinienne, des empreintes digitales ou de l'iris.

EN QUOI L'AUTHENTIFICATION À DEUX FACTEURS DIFFÈRE-T-ELLE DE L'AUTHENTIFICATION MULTIFACTEUR?

Vous avez peut-être entendu parler de la méthode d'authentification appelée l'authentification à deux facteurs (A2F). Ce type d'authentification fait appel à une combinaison de **deux** facteurs d'authentification **différents** pour accéder à un dispositif ou un système.

QU'EN EST-IL DE LA VÉRIFICATION EN DEUX ÉTAPES?

La vérification en deux étapes est un processus exigeant deux méthodes d'authentification qui s'appliquent successivement. Contrairement à l'authentification à deux facteurs, la vérification en deux étapes peut utiliser **le même type de facteur** (c.-à-d., deux clés physiques ou deux données biométriques). On l'appelle parfois l'authentification en deux étapes.

QUELS SONT LES « MEILLEURS » FACTEURS À UTILISER?

Votre organisation doit protéger ses réseaux, ses systèmes et son information. Elle doit également s'assurer que ses employés peuvent utiliser les systèmes et accéder à l'information dont ils ont besoin dans l'exercice de leurs fonctions. Par conséquent, ce qui constitue la meilleure solution d'authentification multifacteur diffère d'une organisation à l'autre. Par exemple, si votre organisation ne permet pas l'utilisation de clés USB, il pourrait être difficile d'avoir recours à un jeton matériel. Il serait alors préférable d'utiliser une phrase de passe ou des données biométriques.

Votre organisation doit déterminer quelles stratégies d'authentification des utilisateurs répondent le mieux à ses exigences en matière de sécurité, puis informer tous les utilisateurs de l'approche qu'elle a adoptée en matière d'authentification multifacteur.

Il faut se rappeler qu'une fois mise en œuvre, toute combinaison de ces facteurs d'authentification permettra de renforcer la posture de cybersécurité dans son ensemble.

SÉRIE SENSIBILISATION

QUELS AUTRES FACTEURS DOIT-ON ENVISAGER AU MOMENT DE METTRE EN PLACE L'AUTHENTIFICATION MULTIFACTEUR?

Il peut être difficile de trouver les options d'authentification multifacteur sur un dispositif ou dans un compte. Elles sont souvent dissimulées dans les paramètres avancés d'un service.

Votre organisation doit établir un plan de récupération clair advenant la perte ou la compromission des facteurs d'authentification. À titre d'exemple, un utilisateur qui perd son jeton ne sera plus en mesure d'accéder à son compte. Les utilisateurs devraient donc pouvoir s'adresser au centre d'assistance afin d'obtenir un jeton matériel de rechange, lequel sera alors remplacé par un nouveau.

Si l'authentification multifacteur n'est pas offerte par un des services importants utilisés par votre organisation, il serait bon de chercher un service de remplacement. S'il n'en existe aucun, vos employés et vous devriez vous montrer encore plus vigilants au moment de créer des phrases de passe ou des mots de passe. Pour plus de conseils à ce sujet, consultez le document ITSAP.30.32, *Pratiques exemplaires de création de phrases de passe et de mots de passe*.

L'authentification multifacteur vous permet d'utiliser un mot de passe plus court, puisque l'authentification additionnelle ajoute une autre couche de protection. Il est toutefois recommandé d'utiliser une phrase de passe ou un mot de passe d'une longueur minimale de 6 à 8 caractères.

Si un dispositif ou un compte contient des données hautement sensibles, il pourrait être préférable d'utiliser trois facteurs d'authentification (dont des données biométriques). Il faut garder à l'esprit que bien que vos données biométriques vous soient uniques, des auteurs de menace peuvent les imiter, les copier ou les reproduire.

La mise en œuvre de l'authentification multifacteur peut nécessiter des coûts élevés et bien des efforts. Cela dit, advenant une compromission, les coûts et les efforts nécessaires pour reprendre vos activités à la suite d'une attaque pourraient être beaucoup plus élevés.

AUTRES POINTS À SE RAPPELER

En conclusion, votre organisation doit s'assurer qu'elle :

- connaît la valeur de son information et sait où est stockée l'information à valeur élevée;
- choisit des services (d'infonuagique et Internet) qui offrent l'authentification multifacteur;
- encourage les utilisateurs et les administrateurs à faire appel à l'authentification multifacteur pour les services d'infonuagique et Internet, particulièrement si ces services contiennent des données sensibles;
- fait preuve de vigilance lorsqu'elle a recours à des services avec authentification à un seul facteur;.
- utilise des phrases de passe ou des mots de passe complexes si l'authentification à un seule facteur et utilisé.

OÙ PUIS-JE TROUVER DE LA DOCUMENTATION SUR L'AUTHENTIFICATION MULTIFACTEUR?

Le Centre canadien pour la cybersécurité a publié d'autres ouvrages sur le sujet, dont les suivants :

- ITSAP.00.019, *Biométrie*;
- ITSAP.30.32, *Pratiques exemplaires de création de phrases de passe et de mots de passe*;
- ITSAP.00.001, *Utiliser son dispositive mobile en toute sécurité*

Avez-vous besoin d'aide ou des questions? Vous voulez tout savoir sur la cybersécurité?
Visitez le site Web du Centre canadien pour la cybersécurité à **cyber.gc.ca**.