Sécurisez vos comptes et vos appareils avec une authentification multifacteur

CANADIAN CENTRE FOR CYBER SECURITY

Février 2024 | ITSAP.30.030

Tant les organisations que les personnes peuvent tirer avantage de l'authentification multifacteur (AMF) pour sécuriser leurs dispositifs et leurs comptes. Si l'AMF est activée, 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'AMF propose une couche de protection supplémentaire contre les cyberattaques, comme une attaque par bourrage d'identifiants. Dans le cas d'une attaque par bourrage d'identifiants, les pirates informatiques utilisent des justificatifs d'identité précédemment volés d'un service en ligne, en espérant que vous utilisiez les mêmes justificatifs sur d'autres services. Si ce n'est pas déjà le cas, il est fortement recommandé à votre organisation et à vous d'avoir recours à l'AMF, dans la mesure du possible, pour protéger vos données et vos services opérationnels à valeur élevée contre les auteures et auteurs de menace.

Facteurs d'authentification

L'AMF emploie une combinaison des facteurs suivants pour authentifier une utilisatrice ou un utilisateur :

- **Quelque chose que vous connaissez :** Généralement, votre phrase de passe, votre mot de passe ou votre numéro d'identification personnel (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 une application d'authentification ou un texte;

- **Quelque chose qui vous caractérise :** Ce facteur repose sur une caractéristique biométrique unique comme la lecture d'empreintes rétiniennes, d'empreintes digitales, de l'iris ou de la structure faciale.

Authentification à deux facteurs et validation en deux étapes

L'**authentification à deux facteurs** (A2F) est un type d'AMF qui fait appel à une combinaison de **deux** facteurs d'authentification **différents** pour accéder à un dispositif ou à un système.

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**, comme deux clés physiques ou deux données biométriques. On l'appelle parfois l'authentification en deux étapes.

Quels sont les « meilleurs » facteurs à utiliser?

Une organisation doit protéger ses réseaux, ses systèmes et son information. Elle doit également s'assurer que les membres de son effectif peuvent utiliser les systèmes et accéder à l'information dont elles et ils ont besoin dans l'exercice de leurs fonctions. C'est pourquoi les meilleures solutions d'AMF varient d'une organisation à une autre. Par exemple, si une organisation ne permet pas l'utilisation de clés USB, il serait impossible 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 répondent le mieux à ses exigences en matière de sécurité, puis informer toutes les utilisatrices et tous les utilisateurs de l'approche qu'elle a adoptée en matière d'AMF.

Une fois mise en œuvre, toute combinaison de ces facteurs d'authentification permettra de renforcer la posture de cybersécurité dans son ensemble.

Vulnérabilités liées à l'AMF

L'AMF aide à protéger les comptes de votre organisation, mais elle n'est pas infaillible. Les auteures et auteurs de menace utilisent diverses techniques pour tenter de contourner cette protection, comme les **attaques par demande d'authentification répétée**, le **vol de jeton** et les **attaques par interception**.

- Attaque par demande d'authentification répétée : Il s'agit d'une technique permettant aux auteures et auteurs de menace d'inonder une utilisatrice ou un utilisateur de notifications jusqu'à l'inciter à en accepter une.
- Vol de jeton : Les jetons permettent de partager des données entre une utilisatrice ou un utilisateur et un système. Si une ou un auteur de menace vole un jeton, il lui est alors possible d'accéder à des données protégées dans la session.
- Attaque par interception : Il s'agit d'une technique permettant aux auteures et auteurs de menace d'intercepter et de modifier des données envoyées entre une utilisatrice ou un utilisateur et une plateforme. Cette technique repose souvent sur le recours à de faux liens URL ou textos conçus de manière à ce qu'ils semblent provenir du système légitime.

Communications Security Establishment | Centre de la sécurité des télécommunications

Canada

Solutions de sécurité supplémentaires

Afin d'atténuer les vulnérabilités associées aux attaques par demande d'authentification répétée et à l'hameçonnage, vous pouvez mettre en œuvre les solutions ci-dessous.

Activez la mise en correspondance des nombres dans les configurations d'AMF : Cette fonction invite l'utilisatrice ou utilisateur à saisir des nombres autorisés sur la plateforme d'identification afin de terminer le processus d'authentification. Elle peut aider à lutter contre les attaques par demande d'authentification répétée.

Mettez en place des technologies d'AMF résistantes à l'hameçonnage : Par exemple, nous recommandons fortement d'utiliser les solutions fondées sur FIDO (*Fast Identity Online*) pour sécuriser les comptes en ligne. Consultez la publication de la Cybersecurity and Infrastructure Security Agency sur l'AMF résistante à l'hameçonnage (en anglais seulement).

Restreignez le nombre de demandes d'AMF par utilisatrice ou utilisateur : Tirez parti de cette fonction si elle est offerte par votre solution d'AMF, car elle peut vous aider à protéger vos comptes contre une attaque par demande d'authentification répétée.

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 les activités à la suite d'une attaque pourraient être beaucoup plus élevés.

Facteurs à considérer lors de l'utilisation de l'AMF

Les options d'AMF sont souvent dissimulées dans les paramètres avancés d'un service et difficiles à trouver. L'organisation doit offrir de la formation ou de l'information aux utilisatrices et utilisateurs pour qu'ils sachent comment repérer les paramètres d'AMF et comment les activer conformément à la politique sur l'authentification multifacteur de l'organisation.

Les organisations doivent établir un plan de récupération clair advenant la perte ou la compromission des facteurs d'authentification. À titre d'exemple, une utilisatrice ou un utilisateur qui perd son jeton ne sera plus en mesure d'accéder à son compte. Les utilisatrices et 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. Lorsque ce jeton de rechange est utilisé, il faut le remplacer et l'entreposer dans un coffre-fort ou au bureau d'assistance.

Si vous pensez acheter ou renouveler un service pour votre organisation, tenez compte des options d'AMF proposées par ce service. Si aucune option d'AMF n'est offerte, il faudra que les membres du personnel fassent preuve **d'autant plus de vigilance** au moment de créer des phrases de passe ou des mots de passe. Pour plus de conseils à ce sujet, consultez le document *Pratiques exemplaires de création de phrases de passe et de mots de passe* (ITSAP.30.032).

L'AMF 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 un mot de passe contenant au moins 12 caractères et, si possible, une phrase de passe d'au moins 4 mots et 15 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 les données biométriques soient uniques à une personne, des auteures et auteurs de menace peuvent les imiter, les copier ou les reproduire.

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;
- oblige les utilisatrices et utilisateurs et les administratrices et administrateurs à faire appel à l'authentification multifacteur pour les services d'infonuagique et Internet, particulièrement si ces services contiennent des données sensibles;
- restreint le nombre de services n'autorisant que l'authentification à un facteur.

Pour en savoir plus

Le Centre pour la cybersécurité et ses partenaires ont créé d'autres publications sur le sujet. En voici quelques-unes.

- Biométrie (ITSAP.00.019)
- Pratiques exemplaires de création de phrases de passe et de mots de passe (ITSAP.30.032)
- Utiliser son dispositif mobile en toute sécurité (ITSAP.00.001)
- Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information (ITSP.30.031)
- Étapes à suivre pour déployer efficacement l'authentification multifacteur (ITSAP.00.105)
- Authentication methods: choosing the right type (NCSC) (en anglais seulement)
- Implementing Number Matching in MFA Applications (CISA) (en anglaise seulement)

Communications Security Establishment
Centre de la sécurité des télécommunications
Canada

 No de cat.D97-1/30-030-2024F-PDF ISBN 978-0-660-68432-1