Étapes à suivre pour déployer efficacement l'authentification multifacteur (AMF)

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Mai 2023 | ITSAP.00.105

Les auteurs de menace exploitent fréquemment les justificatifs d'identité faibles ou volés pour compromettre des comptes, ils peuvent ainsi s'introduire dans votre réseau, prendre le contrôle de vos systèmes et obtenir l'accès à votre information sensible. Pour accroître la résilience de votre organisation contre ces cyberattaques, il convient d'utiliser des mécanismes d'authentification robustes, principalement l'authentification multifacteur (AMF), afin de sécuriser les comptes et les appareils sur vos réseaux. L'AMF peut offrir une sécurité accrue dans un environnement sur site, en nuage ou hybride.

L'AMF exige au moins deux facteurs d'authentification différents pour vérifier l'identité de l'utilisatrice ou utilisateur pendant le processus de connexion. Ces facteurs d'authentification peuvent être une combinaison des éléments suivants: quelque chose que l'on connaît (p. ex. un mot de passe ou un NIP), quelque chose que l'on possède (p. ex. une carte à puce ou une clé de sécurité) ou quelque chose qui nous caractérise (p. ex. les caractéristiques biométriques, comme le balayage de l'empreinte digitale ou du visage). Lorsque l'AMF est combinée à d'autres contrôles de sécurité, elle permet de garantir que seules les personnes autorisées pourront accéder aux ressources adéquates. La présente peut aider votre organisation à déployer efficacement l'AMF comme couche supplémentaire de sécurité afin de réduire la probabilité d'occurrence des attaques de justificatifs d'identité compromis ou des fuites de données.

Pratiques exemplaires relatives au déploiement de l'AMF

Afin de garantir le succès du déploiement de l'AMF, vous devez élaborer un plan. Vous devez d'abord consulter les parties prenantes de l'ensemble de votre organisation et identifier les actifs organisationnels (actifs ayant une grande valeur opérationnelle ou données et systèmes sensibles) que vous devez protéger. Vous devez également vous assurer que vous comprenez les répercussions négatives qu'aura la mise en œuvre d'une solution d'AMF sur vos utilisatrices et utilisateurs afin que vous puissiez planifier de façon proactive des mesures d'atténuation. Vous pouvez ensuite sélectionner une solution d'AMF qui répond à vos exigences organisationnelles et qui peut être adaptée afin de répondre aux besoins de votre organisation à mesure que celle-ci continue à grandir et à évoluer. Il est également possible que votre organisation ait besoin de plus d'une solution d'AMF, entre autres, pour répondre aux divers besoins des différents utilisateurs et utilisatrices (p. ex. les administratrices et administrateurs internes, les utilisatrices et utilisateurs réguliers et les clientes et clients externes). Il est important de noter que les solutions d'AMF ne sont pas toutes identiques. Bon nombre de ces solutions offrent des fonctionnalités différentes et certaines pourraient avoir des mises en œuvre d'AMF plus sécurisées que les autres. Peu importe la solution d'AMF que vous choisissez, votre organisation peut la déployer efficacement en respectant les pratiques exemplaires ci-dessous.

Préparer les utilisatrices et utilisateurs dans le but de minimiser la résistance et d'assurer une meilleure acceptation de l'AMF

- ☐ Effectuer, à l'avance, des campagnes de sensibilisation afin d'expliquer comment l'AMF protégera les comptes et améliorera l'ensemble de la sécurité de l'organisation.
- ☐ Offrir des séances de formation aux utilisatrices et utilisateurs pour les aider à mieux comprendre les nouvelles méthodes d'authentification.
- ☐ Sensibiliser les utilisatrices et utilisateurs à l'identification, au signalement et à l'atténuation des attaques par piratage psychologique, comme de l'hameçonnage et du pollupostage d'AMF. Le pollupostage d'AMF, parfois appelé "attaque par demande d'authentification répétée", est une technique permettant aux auteurs de menace d'inonder les victimes éventuelles de notifications envoyées à un téléphone, à un courriel ou à une plateforme de messagerie afin de les inciter à accepter l'invite d'AMF. Les utilisatrices et utilisateurs devraient être formés pour pouvoir repérer ce type d'attaque et le signaler à leur équipe responsable des TI le plus tôt possible.

Planifier un déploiement progressif afin d'améliorer la cybersécurité de l'organisation le plus tôt possible

- ☐ Appliquer d'abord l'AFM aux comptes qui sont des cibles de grande valeur pour les auteurs de menace dans le but d'assurer la protection contre l'utilisation inappropriée des comptes privilégiés et des communications opérationnelles importantes. Cela inclut les comptes d'administrateur et les comptes de courriel des membres de la haute direction.
- ☐ Considérer le déploiement à un groupe pilote d'utilisatrices et utilisateurs ayant des niveaux d'accès de sécurité différents. Utiliser les leçons apprises du projet pilote pour améliorer le plan final de déploiement au reste de l'organisation.

Élaborer des stratégies d'authentification qui répondent aux besoins de l'organisation et à la sensibilité des données

- ☐ Envisager l'utilisation d'AMF pour tous les utilisateurs et utilisatrices, tous les systèmes, toutes les applications (en nuage et sur site) et tous les terminaux sur le réseau. Activer, au minimum, l'AMF pour les comptes associés aux données sensibles comme ceux contenant des rapports financiers et de l'information nominative.
- ☐ Appliquer des contrôles d'accès conditionnel fondés sur les risques pour veiller à ce que des méthodes d'authentification supplémentaires soient requises lorsque le niveau de risque de compromission lié à l'accès d'un système augmente.
- ☐ Comprendre les exigences réglementaires et de conformité de l'organisation et adapter les solutions d'AMF en conséquence.
- ☐ Configurer des stratégies d'AMF fondée sur la session pour les connexions à risques élevés afin d'obliger les utilisatrices et utilisateurs à saisir leurs justificatifs d'identité lorsque leur session expire. Les justificatifs d'identité doivent être constamment validés à chaque connexion.
- ☐ Exiger des facteurs d'authentification supplémentaires en fonction du contexte, comme du rôle, de l'emplacement et du comportement de l'utilisatrice ou utilisateur. Des facteurs d'authentification supplémentaires pourraient également être exigés en fonction du niveau de risque de la tâche prévue. Par exemple, les utilisatrices et utilisateurs travaillant à distance auraient différentes exigences relatives à l'AMF que ceux travaillant sur place.

Préparer l'infrastructure pour le déploiement de l'AMF. Mettre à jour les composants matériels et logiciels, tester les systèmes et veiller à ce que rien n'entrave au bon fonctionnement du système s'il est nécessaire d'apporter des changements à l'AMF.

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada

Étapes à suivre pour déployer efficacement l'authentification multifacteur (AMF)

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ
Mai 2023 | ITSAP.00.105

Choisir les moyens d'AMF adéquats selon le niveau de protection requis

- ☐ Mettre en place une AMF fondée sur le matériel indépendante à l'appareil étant authentifié. Par exemple, nous recommandons fortement d'utiliser les solutions fondées sur FIDO (Fast Identity Online) pour sécuriser les comptes en ligne. Consultez la publication Next Level MFA: FIDO Authentication (en anglais seulement) de la Cybersecurity and Infrastructure Security Agency (CISA) des États-Unis.
- ☐ Exiger l'utilisation d'applications d'authentification, de clés de sécurité ou de cartes à puce comme facteurs d'authentification supplémentaires lorsque les utilisatrices et utilisateurs accèdent au réseau organisationnel au moyen d'un appareil autorisé par l'organisation.
- ☐ Envisager uniquement l'utilisation de codes par message texte en tant que facteur d'authentification pour les connexions à faibles risques. Les messages texte ne sont pas un moyen sécurisé, puisque les codes sont envoyés dans un format non chiffré. De plus en plus de cyberattaques impliquent des auteurs de menace interceptant des codes par message texte au moyen de l'usurpation de carte SIM, de l'hameçonnage ou d'autres attaques par piratage psychologique .

Établir un équilibre entre l'expérience utilisateur et la protection de sécurité pour maximiser la sécurité et minimiser les perturbations

- ☐ Permettre aux utilisatrices et utilisateurs de se servir de différents types de facteurs, dans la mesure du possible, comme des clés de sécurité, des données biométriques ou d'un NIP. Cela permettrait aux utilisatrices et utilisateurs de choisir l'option qui convient le mieux à leurs besoins, ce qui pourrait assurer une meilleure acceptation de l'AMF.
- ☐ Fournir aux utilisatrices et utilisateurs un mécanisme leur permettant de faire part de leur rétroaction liée à l'utilisation d'AMF et être disposé à modifier les stratégies et les procédures de l'organisation afin d'améliorer l'expérience utilisateur. Le mécanisme de rétroaction pourrait permettre de révéler les possibles réticences des utilisatrices et utilisateurs, comme les préoccupations en matière de protection de la vie privée relatives à certains types d'AMF (p. ex. les données biométriques).
- ☐ Mettre en œuvre une AMF combinée à une application d'authentification unique (SSO pour Single Sign-On) afin de connecter automatiquement les utilisatrices et utilisateurs autorisés à leurs comptes connexes. Cette mise en œuvre peut améliorer l'expérience utilisateur, puisque les utilisatrices et utilisateurs passeront moins de temps à se connecter à de multiples comptes chaque jour.
- ☐ Effectuer régulièrement des évaluations de la solution d'AMF afin de veiller à ce qu'elle réponde toujours aux besoins des utilisatrices et utilisateurs et qu'elle protège toujours l'information sensible de l'organisation. Ces évaluations sont importantes, car les technologies de cybersécurité évoluent constamment.

99.9% des compromissions de comptes peuvent être bloquées au moyen de l'AMF

Étude de Microsoft, 2019

Alléger le fardeau des ressources de TI dans le cadre du soutien apporté au déploiement et à la maintenance de l'AMF

- ☐ Offrir aux utilisatrices et utilisateurs une méthode d'AMF de rechange dont le niveau de robustesse est identique à celui de la méthode principale. Mettre en place une façon facile pour les utilisatrices et utilisateurs de réinitialiser eux-mêmes leur AMF au cas où leur méthode d'AMF principale est perdue, indisponible ou compromise.
- ☐ Se servir d'outils de surveillance connexes pour détecter et bloquer automatiquement les addresses IP suspectes qui accèdent au réseau.
- ☐ Activer la journalisation des événements pour les événements d'AMF et surveiller les rapports d'authentification. Cela permettra de détecter les activités anormales qui pourraient mener à la tentative d'exploitation des lacunes dans le processus d'inscription ou de révocation.
- ☐ Se servir d'outils de vérification pour aider au dépannage et à la modification des stratégies d'AMF selon l'utilisation.
- ☐ Permettre aux utilisatrices et utilisateurs de dissocier une clé de sécurité ou un appareil perdu ou volé de leur compte. Cela évite que les auteurs de menace accèdent au compte de l'utilisatrice ou utilisateur si l'appareil volé est intercepté à des fins malveillantes.
- ☐ Configurer des comptes d'urgence pour gérer les activités administratives au cas où les méthodes d'AMF ne sont plus disponibles. Les justificatifs d'identité du compte d'urgence doivent être rigoureusement sécurisés et uniquement utilisés lors du processus de gestion des incidents.

Pour plus d'information, consultez les ressources suivantes:

- Ne mordez pas à l'hameçon: Reconnaître et prévenir les attaques par hameçonnage (ITSAP.00.101)
- Sécurisez vos comptes et vos appareils avec une authentification multifacteur (ITSAP.30.030)
- Pratiques exemplaires de création de phrases de passe et de mots de passe (ITSAP.30.032)
- Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information (ITSP.30.031 v3)
- Authentication methods: choosing the right type (en anglais seulement), du National Cyber Security Centre
- Utiliser une authentification forte (cours en ligne) d'Innovation, Sciences et Développement économique Canada
- More than a Password – Protect Yourself from Malicious Hackers with Multifactor Authentication (en anglais seulement) de la Cybersecurity and Infrastructure Security Agency

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada