CENTRE FOR CYBERSECURITY BELGIUM

AUTHENTIFICATION MULTIFACTEURS (MFA) : GUIDE POUR LES ORGANISATIONS

COMPRENDRE ET METTRE EN ŒUVRE LA MFA POUR UNE MEILLEURE SÉCURITÉ IT

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Table des matières

1. Introduction 3
2. Qu'est-ce que l'authentification multifacteurs et pourquoi est-elle importante ? 3
3. Authentification multifacteurs : une mesure de sécurité essentielle pour les organisations 4
4. Comment mettre en œuvre l'authentification multifacteurs au travail ? 5
   - 4.1 L'authentification multifacteurs pour les applications 7
   - 4.2 Authentification multifacteurs pour l'accès à distance 8
   - 4.3 Principaux éléments à prendre en compte lors du choix d'une solution MFA 8
   - 4.4 Mettre en œuvre la MFA dans Azure Cloud 9
   - 4.5 Mettre en œuvre la MFA dans Google Cloud 9
   - 4.6 Mettre en œuvre la MFA dans des applications personnalisées avec Itsme 10
   - 4.7 Applications d'authentification 10
5. Considérations relatives à la configuration de l'authentification multifacteurs et au support des utilisateurs 11
6. Problèmes et obstacles potentiels 11
   - 6.1 Perte de connectivité 11
   - 6.2 Facteurs à prendre en compte lors du choix d'une méthode MFA 12
   - 6.3 MFA et BYOD 12
7. Considérations clés pour une utilisation sécurisée de la MFA 13
8. Références 14
   - 8.1 Cyberfondamentaux 14
   - 8.2 Safeonweb (@work) 14

1. Introduction

En matière de sécurisation de vos comptes, vous avez probablement entendu parler de l'authentification à deux facteurs (2FA) ou de l'authentification multifacteurs (MFA). L'authentification à deux facteurs est une approche de sécurité qui exige d'utiliser deux facteurs d'authentification pour accéder à un compte. L'authentification multifacteurs (MFA) nécessite de présenter deux ou plusieurs preuves, ou facteurs, pour s'authentifier. Ainsi, alors que la 2FA implique deux étapes de vérification, la MFA va plus loin en incorporant plusieurs méthodes d'authentification.

Cette solution simple mais forte ajoute une couche supplémentaire de protection en vous demandant de fournir au moins deux formes d'identification. Même si quelqu'un connaît votre mot de passe, la MFA empêche tout accès non autorisé à vos comptes. Il est fortement recommandé d'activer la MFA dès que possible en raison de sa simplicité et de la sécurité accrue qu'elle offre. On ne saurait trop insister sur l'importance de la 2FA et de la MFA pour les organisations, qu'elles soient publiques ou privées. Les cybermenaces, notamment les attaques par ransomware, les violations de données et les intrusions, engendrent des risques considérables. Les statistiques montrent que la la MFA pourrait permettre d'éviter un large pourcentage d'attaques par ransomware. Un grand nombre de ces attaques pourraient être évitées grâce à des mesures d'authentification robustes. En ajoutant plusieurs couches de sécurité, la MFA complique considérablement l'accès aux données sensibles des cybercriminels, réduisant ainsi la probabilité de violations de données et d'autres cybermenaces.

Dans ce guide, nous vous présenterons les principes de base de la MFA et vous dispenserons des conseils pratiques concernant la mise en place de celle-ci au sein de votre organisation. Nous exposerons également des exemples concrets et partagerons des trucs et astuces pour vous aider à ne pas tomber dans les pièges les plus courants lors du déploiement de solutions MFA. Une fois votre lecture achevée, vous disposerez d'une meilleure compréhension de la MFA et de la manière de l'utiliser efficacement pour protéger les informations sensibles de votre organisation. Dans notre Cyberfundamentals Framework, nous soulignons aussi clairement le rôle critique des mesures d'authentification forte dans la protection des actifs numériques de votre organisation.

2. Qu'est-ce que l'authentification multifacteurs et pourquoi est-elle importante ?

En résumé, la MFA implique l'utilisation d'un code ou d'une confirmation supplémentaire en plus de votre mot de passe pour accéder en toute sécurité à un compte ou à un système. La MFA nécessite de fournir un mot de passe et un token ou des données biométriques pour accéder aux informations, ce qui réduit considérablement le risque d'accès non autorisé. En exigeant plusieurs formes d'authentification, la MFA renforce considérablement la sécurité de votre organisation et **réduit le risque d'accès non autorisé à des informations ou à des systèmes sensibles.**

Pour accéder à votre compte en toute sécurité, vous devez prouver votre identité. Pour ce faire, trois méthodes ou facteurs s'offrent à vous :

- une donnée que vous êtes seul à connaître (votre mot de passe ou votre code PIN) ;
- un élément auquel vous seul avez accès (votre téléphone ou votre token) ; ou
- un élément qui fait partie de vous (votre empreinte digitale, votre visage, votre iris, etc.).

La mise en œuvre de la MFA au niveau de l'organisation signifie que les collaborateurs et tout autre utilisateur qui a besoin d'accéder à vos ressources doivent fournir plus d'une forme d'authentification pour accéder aux systèmes et réseaux de l'entreprise, ainsi qu'aux informations et applications sensibles. La MFA peut être appliquée à toute une série d'applications et de systèmes, comme les boîtes mails, les VPN, les services cloud et les réseaux internes.

La MFA gagne en importance dans l'environnement professionnel actuel, où les cybermenaces sont de plus en plus sophistiquées et fréquentes. Une attaque par phishing qui incite un utilisateur à divulguer son mot de passe serait par exemple moins efficace contre un **système utilisant la MFA**, car le pirate informatique devrait également fournir le token ou les données biométriques de la victime pour obtenir l'accès désiré. De même, une attaque par force brute qui tente de multiples combinaisons de mots de passe serait beaucoup moins efficace contre un système utilisant la MFA, puisque, une nouvelle fois, le pirate informatique devrait fournir une forme d'authentification supplémentaire.

Si la MFA **améliore la sécurité** des organisations, elle peut également les aider à **se conformer aux exigences légales et réglementaires** (par exemple le RGPD et la loi NIS2) en matière de mesures d'authentification forte. La MFA peut également contribuer à assurer la continuité des activités en prévenant ou en atténuant l'impact des failles de sécurité, ce qui permet aux organisations de continuer à fonctionner avec un minimum de perturbations.

3. Authentification multifacteurs : une mesure de sécurité essentielle pour les organisations

Alors que la MFA est traditionnellement associée aux grandes entreprises, elle devient aujourd'hui **plus accessible et plus abordable** pour les organisations de toutes tailles. En outre, certaines solutions MFA sont disponibles **sous forme d'abonnement**, ce qui peut aider les organisations à gérer leurs coûts plus efficacement en payant uniquement pour ce dont elles ont besoin. En termes de complexité, les solutions MFA deviennent de plus en plus **conviviales** et **faciles à mettre en œuvre**, de nombreux fournisseurs proposant des options simples et prêtes à l'emploi qui ne nécessitent qu'une configuration minimale.

Certaines solutions MFA s'intègrent même aux systèmes de gestion d'accès existants, comme Active Directory ou LDAP, ce qui permet aux organisations de les adopter plus facilement **sans apporter de changements majeurs à leur infrastructure existante**. LDAP et Active Directory sont tous deux utilisés pour l'authentification et l'autorisation, ce qui permet aux organisations de contrôler l'accès des utilisateurs aux systèmes, aux applications et aux données. En intégrant des solutions MFA à LDAP ou Active Directory, les organisations peuvent améliorer leur sécurité et se protéger contre les cybermenaces, sans avoir besoin de modifier drastiquement leur infrastructure existante. En faisant de la MFA une **mesure de sécurité essentielle**, les entreprises peuvent s'assurer qu'elles prennent des mesures proactives pour protéger leurs activités et les informations sensibles de leurs clients. Globalement, les organisations peuvent mettre en œuvre la MFA pour améliorer leur sécurité et réduire le risque d'accès non autorisé à des informations ou des systèmes sensibles.

En faisant de la MFA une **mesure de sécurité essentielle**, les entreprises peuvent s'assurer qu'elles prennent des mesures proactives pour protéger leurs activités et les informations sensibles de leurs clients. Globalement, les organisations peuvent mettre en œuvre la MFA pour améliorer leur sécurité et réduire le risque d'accès non autorisé à des informations ou des systèmes sensibles.

Pourquoi un seul mot de passe ne suffit plus :

- Les mots de passe sont faciles à deviner, surtout s'ils sont simples et aisés à retenir. C'est pourquoi de nombreux pirates utilisent des attaques par force brute et par pulvérisation de mots de passe, qui consistent à essayer de deviner un mot de passe en testant de nombreuses combinaisons jusqu'à obtenir le bon résultat.
- Un même mot de passe peut être utilisé pour plusieurs comptes, ce qui signifie que si un mot de passe est compromis, les pirates peuvent l'utiliser pour accéder à d'autres comptes. Cela s'appelle la réutilisation des mots de passe et il s'agit d'un problème courant qui rend l'authentification par mot de passe moins sûre.

Les mots de passe peuvent être **volés par le biais d'attaques de phishing ou de malwares.** Les pirates informatiques peuvent envoyer de faux mails ou messages qui semblent provenir d'une source légitime, incitant les utilisateurs à partager leurs identifiants de connexion. De même, des malwares peuvent être utilisés pour voler les mots de passe directement à partir de l'appareil de l'utilisateur.

Au vu de ces faiblesses, **l'utilisation de mots de passe uniquement élargit le champ des menaces.** Les pirates peuvent par exemple utiliser des mots de passe volés ou devinés pour accéder aux données ou systèmes sensibles d'une organisation. Ils peuvent également utiliser des outils pour craquer des mots de passe faibles, puis utiliser les mêmes mots de passe pour accéder à d'autres comptes. En résumé, les faiblesses des mots de passe les rendent vulnérables à l'exploitation et la MFA est se révèle un allié crucial pour renforcer la sécurité.

4. Comment mettre en œuvre l'authentification multifacteurs au travail ?

En pratique, la mise en œuvre de la MFA dans les organisations comporte quatre étapes pour garantir l'efficacité et la sécurité du déploiement : l'identification, le choix, la planification et la mise en œuvre.

La première étape consiste à **identifier les systèmes et les applications qui nécessitent la MFA,** ainsi que les types d'authentification les plus appropriés. L'accès aux données confidentielles doit être sécurisé par une solution MFA.

La deuxième étape consiste à **choisir une solution MFA adaptée aux besoins et au budget de votre organisation.** Lorsqu'elles choisissent une solution MFA, les organisations doivent prendre en compte des facteurs tels que la facilité d'utilisation, la variabilité s'échelle et le coût. Vous devriez également choisir une solution compatible avec les systèmes et applications que votre organisation utilise, tout en prenant compte des risques et menaces de sécurité auxquels votre organisation est exposée.

La troisième étape consiste **à planifier le déploiement de la solution MFA.** Cette étape est importante pour garantir un déploiement efficace, qui ne perturbe pas les activités de l'entreprise. Les organisations doivent également prendre en compte des éléments tels que la formation des utilisateurs, la communication et le support lors de la planification du déploiement. Il est important de communiquer les avantages de la MFA aux utilisateurs et de les former à l'utilisation correcte de la solution MFA.

Voici quelques exemples spécifiques que les organisations peuvent prendre en considération au moment de choisir une solution MFA :

- **MFA basée sur les SMS :** un code à usage unique est envoyé par SMS à l'utilisateur, qui saisit ensuite le code pour compléter le processus d'authentification.
- **MFA basée sur un logiciel :** Une application mobile ou un logiciel de bureau génère un code à usage unique. Google Authenticator et Microsoft Authenticator sont des exemples de MFA basée sur un logiciel.
- **MFA basée sur un élément matériel :** Cette option implique généralement un token physique, comme une carte à puce ou un dispositif USB, qui génère un code à usage unique. Ce type de MFA peut s'avérer plus coûteuse et moins souple que les autres options, mais peut convenir aux organisations qui ont besoin d'un niveau de sécurité plus élevé.
- **MFA biométrique :** Des données biométriques, telles que les empreintes digitales ou la reconnaissance faciale, sont utilisées pour authentifier les utilisateurs. La MFA biométrique peut s'avérer plus pratique et plus sûre que les autres options, mais nécessiter du matériel ou des logiciels spécialisés et donc être plus coûteuse.

La dernière étape consiste en la **mise en œuvre de la solution MFA.** Elle implique de configurer la solution MFA pour qu'elle fonctionne avec les systèmes et les applications qui en ont besoin. Les organisations doivent également fournir un soutien continu aux utilisateurs pour s'assurer que la solution MFA est utilisée correctement et pour résoudre les problèmes éventuels.

Renforcer la cybersécurité peut souvent sembler une tâche colossale et complexe, en particulier avec des ressources et des budgets limités. Cependant, mettre en œuvre un solution MFA peut être un moyen rapide et efficace d'améliorer de manière significative votre sécurité. Cette couche de sécurité supplémentaire réduit considérablement le risque d'accès non autorisé, car elle complique la tâche des pirates informatiques puisqu'ils ne peuvent pas simplement contourner les mesures de sécurité traditionnelles basées sur les mots de passe. La MFA est facile à mettre en œuvre, de nombreux fournisseurs proposant des solutions conviviales. En optant pour cette solution, les organisations peuvent rapidement améliorer leur sécurité, protéger leurs données sensibles et accroître la confiance de leurs clients, tout en restant dans les limites de leur budget et de leurs ressources.

4.1 L'AUTHENTIFICATION MULTIFACTEURS POUR LES APPLICATIONS

La MFA peut être appliquée à toute une série d'applications et de systèmes, comme les boîtes mails, les VPN, les services cloud et les réseaux internes. Les services les plus couramment utilisés proposent une forme de vérification à plusieurs facteurs et disposent d'une page d'instruction concise. En voici quelques exemples :

- Dropbox
- Google
- LinkedIn
- Microsoft
- Skype
- WhatsApp
- Yahoo

Vous trouverez davantage d'exemples plus concrets dans l'article suivant : L'authentification à deux facteurs, comment faire?

4.2 AUTHENTIFICATION MULTIFACTEURS POUR L'ACCÈS À DISTANCE

L'accès à distance désigne la capacité des utilisateurs ou des processus agissant en leur nom à se connecter à un système d'information organisationnel **par le biais de réseaux externes tels qu'Internet.** Cet accès est généralement facilité par des technologies telles que les Virtual Private Networks (VPN) cryptés pour garantir la confidentialité et l'intégrité de la communication. La mise en œuvre d'un accès à distance sécurisé implique de mettre en place des restrictions d'utilisation, des exigences de configuration et des protocoles d'autorisation stricts avant d'autoriser de telles connexions. Cela garantit que seuls les utilisateurs autorisés accèdent au système à distance, protégeant ainsi le système contre toute menace extérieure éventuelle.

On ne saurait trop insister sur l'importance de la MFA dans ce contexte. Des cybercriminels déterminés parviendront toujours à craquer, deviner ou extorquer un mot de passe unique, aussi complexe soit-il. En mettant en œuvre le MFA, les entreprises ajoutent une couche de sécurité supplémentaire à leurs protocoles d'accès à distance, garantissant que seuls les utilisateurs autorisés accèdent à leurs systèmes.

4.3 PRINCIPAUX ÉLÉMENTS À PRENDRE EN COMPTE LORS DU CHOIX D'UNE SOLUTION MFA

Avant de choisir une solution MFA, il convient de garder à l'esprit les considérations suivantes :

- **Sécurité :** choisissez un outil MFA sécurisé qui respecte les normes et les meilleures pratiques en matière de sécurité ;
- **Compatibilité :** choisissez un outil FMA compatible avec le système et l'infrastructure existants au sein de votre organisation (par exemple, la version du système d'exploitation) et qui peut être facilement intégré au cadre d'authentification de votre organisation (par exemple, Active Directory) ;
- **Déploiement :** choisissez un outil MFA qui assure la sécurité et qui soit facile à déployer dans l'environnement de votre organisation, et pensez au niveau de soutien nécessaire ;
- **Coût :** évaluez le coût des ressources nécessaires à la mise en œuvre de la MFA, telles que la maintenance, les frais de licence, etc.
- **Options d'authentification :** il est préférable de choisir un outil MFA offrant une variété d'options d'authentification afin de permettre aux utilisateurs de choisir les facteurs d'authentification en fonction de leurs préférences et de leurs besoins.

Vous trouverez ci-dessous quelques exemples de mise en place de l'authentification multifactoreurs au sein de votre organisation à l'aide des applications d'authentification les plus courantes. Il s'agit de lignes directrices générales qui peuvent ne pas correspondre aux besoins de votre organisation ou varier selon les spécificités de votre environnement.

4.4 METTRE EN ŒUVRE LA MFA DANS AZURE CLOUD

Étape 1 : Azure Active Directory (pré-requis)

Afin de pouvoir utiliser l'application Microsoft authenticator, votre organisation doit disposer d'un compte Azure AD (Active Directory).

Étape 2 : Activer la MFA

Chaque édition d'Azure AD inclut la MFA Azure AD. Aucune licence supplémentaire n'est nécessaire pour une campagne d'enregistrement. Cela peut être fait sur le portail Azure (Azure Active Directory > Security > MFA).

Étape 3 : Choisir des méthodes d'authentification

Microsoft authenticator prend en charge une série de méthodes d'authentification, telles que les notifications push et les codes à usage unique.

Étape 4 : Configurer des politiques

Cette étape permet à votre organisation de déterminer quels utilisateurs doivent utiliser la MFA, quelles méthodes d'authentification peuvent être utilisées et quand la MFA est requise (pour une application spécifique, etc.).

L'une des politiques suivantes peut être utile :

- *MFA Registration Policy*: Les utilisateurs devront être autorisés à recevoir des notifications via l'application mobile.
- *Authentication Methods Policy*: Les utilisateurs devront être autorisés à utiliser l'application Authenticator et le mode d'authentification devra être défini sur « Any » ou « Push ».

Étape 5 : Paramétrer Microsoft authenticator

Une fois que la MFA est activée et que les politiques sont configurées, les instructions relatives à la configuration de l'authentification Microsoft peuvent être communiquées aux utilisateurs par mail ou en utilisant les plateformes de communication internes de votre organisation, comme l'intranet.

Pour plus de conseils :

- Inciter les utilisateurs à configurer Microsoft Authenticator - Microsoft Entra | Microsoft Learn
- Configurer la politique d'enregistrement MFA - Azure Active Directory Identity Protection - Microsoft Entra | Microsoft Learn

4.5 METTRE EN ŒUVRE LA MFA DANS GOOGLE CLOUD

Étape 1 : Compte Google Cloud (pré-requis)

Pour utiliser Google Authenticator, votre organisation doit disposer d'un compte Google Cloud pour le déploiement de la MFA.

Étape 2 : configurer la vérification en deux étapes

Activez la vérification en deux étapes à l'aide de la Google Admin Console :

Menu > Security > Authentication > 2-step verification.

Étape 3 : choisir la méthode d'authentification

Google authenticator prend en charge toute une série de méthodes d'authentification pour la vérification en deux étapes, telles que l'application Google authenticator (pour les versions Android 4.4 et supérieures), les clés de sécurité, Google prompt, les sms, les appels téléphoniques et les codes back-up.

Étape 4 : configurer les politiques

Déterminez les utilisateurs qui doivent utiliser la MFA. Pour appliquer le paramètre à tout le monde, sélectionnez l'unité organisationnelle supérieure. Sinon, sélectionnez une unité inférieure ou un groupe de configuration et cochez la case Autoriser les utilisateurs à activer la vérification en deux étapes.

Pour appliquer la MFA à tous les utilisateurs ou au groupe sélectionné, activez l'option d'exécution.

Étape 5 : implémenter la vérification en deux étapes

Fournissez des instructions pour la mise en place de Google authenticator aux utilisateurs par mail ou par le biais des plateformes de communication interne de votre organisation.

Pour plus de conseils : Déployer la validation en deux étapes - Google Workspace Admin Help

4.6 METTRE EN ŒUVRE LA MFA DANS DES APPLICATIONS PERSONNALISÉES AVEC ITSME

Étape 1 : s'enregistrer pour les services MFA d'Itsme

Votre organisation doit être enregistrée pour les services MFA d'itsme afin d'activer le MFA en utilisant l'application itsme et de créer un compte sur le portail d'administration d'itsme permettant à votre organisation de gérer les paramètres MFA et de consulter les statistiques d'utilisation.

Étape 2 : choisir la méthode d'authentification

Les méthodes d'authentification disponibles dans itsme reposent au moins sur la combinaison d'un élément que l'utilisateur possède, comme son smartphone et l'application itsme installée, et les données biométriques de l'utilisateur, comme l'empreinte digitale ou Face ID, ou une donnée que l'utilisateur connaît (par exemple, un code PIN).

Étape 3 : Configurer les politiques

Parcourez les paramètres dans le portail d'administration et sélectionnez les règles qui détermineront quand la MFA Itsme est nécessaire, les exceptions et la notification de configuration en cas d'échec des tentatives d'ouverture de session.

Étape 4 : mettre la MFA Itsme en œuvre

Fournissez des instructions pour la mise en place d'Itsme aux utilisateurs par mail ou par le biais des plateformes de communication interne de votre organisation.

Pour plus de conseils : General information - Documentation - Onboarding (belgianmobileid.be)

4.7 APPLICATIONS D'AUTHENTIFICATION

Une application d'authentification est une application utilisée pour générer des mots de passe à usage unique basés sur le temps (TOTPS) pour l'authentification multifactorielle. Elle aide les utilisateurs à sécuriser leurs comptes en fournissant une deuxième couche de vérification.

- Authy
- Google Authenticator

- Microsoft Authenticator
- Okta Verify

5. Considérations relatives à la configuration de l'authentification multifacteurs et au support des utilisateurs

Configuration de politiques :

- Déterminez la méthode d'authentification autorisée fournie par l'application d'authentification choisie et compatible avec l'environnement de votre organisation et les besoins des utilisateurs.
- Il est recommandé d'appliquer l'authentification MFA à tous les utilisateurs et à toutes les applications, en particulier pour le travail à distance. Au cours de ce processus, l'administrateur doit spécifier pour quel utilisateur, groupe et application la MFA est applicable, définir des critères pour les exceptions et s'assurer que les contrôles appropriés sont en place.
- Intégrer la MFA au système disponible au sein de votre organisation, tel qu'Active Directory, afin de garantir que la MFA est appliquée à toutes les applications et à tous les systèmes, et d'assurer un niveau de sécurité élevé, tout en garantissant une bonne expérience utilisateur grâce à l'utilisation d'un seul ensemble d'informations d'identification.

Soutien aux utilisateurs :

Après la configuration des politiques et la mise en œuvre de la MFA, les utilisateurs ne pourront plus s'authentifier au système, le cas échéant, sans activer la MFA. Votre organisation doit s'assurer que les utilisateurs bénéficient d'un support approprié :

- Communiquez clairement le processus d'activation de la MFA et donnez des lignes directrices aux utilisateurs concernant la configuration de l'application d'authentification dans leurs appareils mobiles, en utilisant les outils de communication de votre organisation tels que les mails et l'intranet.
- Organisez des séances de formation pour les utilisateurs afin de les sensibiliser à la MFA, à son objectif et à ses utilisations possibles.
- Fournissez un support permanent et désignez des personnes de contact auxquelles les utilisateurs peuvent demander de l'aide pour la mise en œuvre.
- Tenez les utilisateurs informés des changements ou des mises à jour des politiques MFA et de leur applicabilité.

6. Problèmes et obstacles potentiels

6.1 PERTE DE CONNECTIVITÉ

Il est important de mettre en place un plan B pour savoir comment agir si les utilisateurs ne parviennent pas à s'authentifier à l'aide de la MFA en cas de perte de connectivité, de perte de l'appareil compatible avec la MFA, ou s'ils ne peuvent pas s'authentifier à l'aide de la méthode principale (par exemple, numéro de GSM bloqué, changement d'adresse mail). Ce plan peut inclure :

- Fournir une **méthode d'authentification de secours** telle qu'un numéro de téléphone ou une adresse mail secondaire.
- Utiliser d'**autres méthodes d'authentification** qui ne reposent pas sur la connectivité (par exemple, des token physiques, des cartes à puce).

- **Désactiver temporairement la MFA** pour un utilisateur ou un groupe d'utilisateurs spécifiques. Cette solution ne doit être utilisée qu'en ultime recours, et la MFA doit être réactivée dès le problème résolut.

En outre, il convient de définir un guide de soutien opérationnel comprenant des instructions étape par étape concernant la manière de résoudre le problème, les personnes à contacter pour obtenir de l'aide et la manière de garantir la sécurité des données de l'organisation pendant la panne.

6.2 FACTEURS À PRENDRE EN COMPTE LORS DU CHOIX D'UNE MÉTHODE MFA

Lorsqu'il s'agit de choisir une méthode d'authentification multifacteurs, il est important d'évaluer le type de MFA qui convient le mieux aux besoins de votre organisation. L'une des méthodes MFA les plus couramment utilisées est une application d'authentification. Bien que cette méthode soit pratique et sûre, il est important de garder à l'esprit que tous les utilisateurs ont besoin d'un smartphone pour l'utiliser. Cela peut poser un problème pour les **organisations qui ne fournissent pas de smartphone à leurs employés** ou **pour les employés qui n'ont pas de smartphone, qui ne veulent pas installer** l'application sur leur smartphone personnel ou qui n'ont qu'un accès limité à celui-ci. Dans ces cas, il peut être nécessaire d'envisager d'autres méthodes MFA, telles qu'un token de sécurité physique ou un système basé sur des SMS, pour s'assurer que tous les utilisateurs peuvent accéder aux systèmes en toute sécurité. Il est donc essentiel de **peser le pour et le contre** des différentes méthodes MFA avant de prendre une décision, et de s'assurer que la méthode choisie est accessible à tous les utilisateurs.

6.3 MFA ET BYOD

Les appareils personnels tels que les smartphones utilisés dans le cadre du travail peuvent ne pas être compatibles avec la méthode MFA choisie par votre organisation, **ce qui complique l'utilisation de la MFA dans un environnement BYOD (Bring Your Own Device)** et la mise en œuvre d'une MFA cohérente sur tous les appareils d'une manière formelle et correcte.

Par conséquent, votre organisation devrait envisager d'utiliser un système de gestion des appareils mobiles (MDM) pour gérer les appareils personnels utilisés par les utilisateurs dans le cadre de leur travail et s'assurer que ces appareils sont correctement sécurisés et conformes aux politiques de sécurité de votre organisation.

En outre, des politiques de sécurité de l'organisation devraient être appliquées afin de :

- Veiller à ce que les **exigences minimales de sécurité** soient mises en œuvre dans les dispositifs des utilisateurs (par exemple, le type de système d'exploitation, l'obligation de maintenir le dispositif à jour avec les correctifs de sécurité, les configurations, etc.)
- Communiquer l'importance de la MFA et le **risque associé à l'utilisation d'appareils personnels** à des fins professionnelles. Elles doivent être communiquées à tous les collaborateurs de l'organisation afin de les sensibiliser à la protection des appareils personnels utilisés à des fins professionnelles.

- Fournir aux utilisateurs un support et des **consignes claires** pour configurer correctement leurs appareils en vue d'une utilisation avec la MFA, ainsi que de procédures indiquant comment et où signaler un incident de sécurité lié à BYOD.
- Limiter l'accès à distance. Votre organisation devrait également envisager de **segmenter l'accès** à ses données et applications en fonction du niveau de risque et d'exiger la MFA dès que possible, en particulier pour les données et applications à haut risque et l'accès à distance.

En conclusion, la mise en œuvre de la **MFA dans un environnement BYOD** doit être considérée comme une mesure de sécurité essentielle, car il se peut que les appareils des collaborateurs ne répondent aux mêmes normes de sécurité que les appareils appartenant à l'entreprise.

7. Considérations clés pour une utilisation sécurisée de la MFA

Lorsque l'on utilise la MFA pour ajouter une couche supplémentaire de protection et renforcer la sécurité, il est important d'être vigilant et de prendre compte en compte certains éléments :

- **Garantir la sécurité des appareils :** effectuez les mises à jour de sécurité et les correctifs pour votre application MFA, les systèmes d'exploitation et les versions logicielles installées sur vos appareils dès qu'ils sont disponibles afin de corriger les éventuelles vulnérabilités.
- **Interaction réfléchie :** si vous choisissez des notifications push up comme deuxième facteur d'authentification, il est important de rester vigilant et d'éviter d'accepter les notifications sans en examiner le contenu. Prenez toujours le temps de lire la notification avant d'agir.
- **Utilisez un mot de passe/une paraphrase fort :** Outre la MFA, utilisez un mot de passe fort et long ou un ensemble d'au moins trois mots communs aléatoires assemblés en une phrase alliant mémorisation et sécurité, avec des caractères minuscules et majuscules, éventuellement des chiffres et des caractères spéciaux, et évitez les solutions évidentes, comme « mot de passe », les séquences de lettres ou de chiffres et les informations personnelles.
- **Utilisez des plateformes officielles :** Lorsque vous téléchargez des applications MFA, utilisez des app stores officiels de confiance tels que Google Play Stores pour Android ou l'Apple App Store pour les appareils IOS afin de garantir l'authenticité et l'intégrité de l'application et de réduire le risque de téléchargement de logiciels malveillants.

8. Références

8.1 CYBERFONDAMENTAUX

Cette annexe renvoie aux cyberfondamentaux associés à l'authentification multifacteurs (MFA), offrant ainsi une référence détaillée pour soutenir la mise en œuvre et la gestion de la MFA dans notre cadre de cybersécurité.

- **PR.AC-3**: **L'accès à distance est géré.**

  Mesure clé : les réseaux de l'organisation accessibles à distance doivent être sécurisés, **notamment par une authentification multifacteurs (MFA).**

8.2 SAFEONWEB (@WORK)

Protéger les comptes grâce à l'authentification multifacteur | Safeonweb@work

Un mot de passe fort pour protéger vos informations précieuses | Safeonweb@work

Access policy | Safeonweb@work

Utilisez l'authentification à deux facteurs | Safeonweb

L'authentification à deux facteurs, comment faire? | Safeonweb