Qu'est-ce que l'authentification à plusieurs facteurs (MFA) ?

L'authentification multiple (Multi-factor authentication en anglais ou MFA) est un système de sécurité qui fait appel à plusieurs méthodes d'authentification, à partir de différentes catégories d'informations d'identification (des preuves), pour vérifier l'identité de l'utilisateur qui souhaite se connecter ou effectuer une transaction.

Ce type d'authentification combine au moins deux informations d'identification indépendantes portant sur ce que l'utilisateur sait (son mot de passe), sur ce qu'il possède et sur ce qu'il est (une vérification biométrique).

La MFA a pour objectif de mettre en place plusieurs niveaux de protection, afin de rendre plus difficile l'accès d'une personne non autorisée à une cible telle qu'un emplacement physique, un appareil informatique, un réseau ou une base de données. Ainsi, même si le pirate parvient à déchiffrer l'un des facteurs, il lui reste encore au moins un obstacle à franchir avant d'atteindre sa cible.

Technologies d'authentification multifacteur :

Token : petits dispositifs matériels portés par l'utilisateur pour obtenir l'accès à un service réseau. Ils peuvent prendre la forme d'une carte à puce ou être intégrés dans un objet facilement transportable, tel qu'un porte-clé ou une clé USB.
Les Token (ou jetons de sécurité) constituent le facteur matériel historique de l'authentification multiple. Cependant, les jetons logiciels deviennent plus courants que les dispositifs matériels.

Tokens logiciels : ces applications génèrent un code PIN de connexion à usage unique.
Les jetons logiciels servent souvent pour l'authentification multiple mobile, dans laquelle c'est l'appareil lui-même (smartphone, par exemple) qui fournit le facteur matériel.

Authentification mobile : il en existe plusieurs variantes, dont les SMS et appels téléphoniques envoyés à un utilisateur en guise de méthode hors bande, les applications

OTP de smartphone, les cartes SIM et cartes à puce sur lesquelles sont stockées des données d'authentification.

Méthodes d'authentification biométrique, parmi lesquelles le balayage de la rétine, le balayage de l'iris, l'analyse de l'empreinte digitale, l'identification des veines du doigt, la reconnaissance faciale, la reconnaissance vocale, la forme de la main ou celle du lobe de l'oreille.

Double factor Athentication 2FA

En quoi consiste la vérification en deux étapes ?

La vérification en deux étapes consiste à la protection des utilisateurs, en bloquant l'accès à votre compte (Microsoft, Azur, Google et compte d'entreprise).

Elle utilise deux formes différentes : votre mot de passe et une méthode de contact (ou informations de sécurité). Même si quelqu'un à connaissance de votre mot de passe, il ne pourra pas aller plus loin s'il n'a pas accès à vos informations de sécurité lié à votre méthode de double authentification.

Exemple :

Une personne à accès à votre compte Microsoft d'une position A, votre smartphone va détecter une anomalie de localisation, et vous demander une authentification pour valider l'authenticité de votre personne avec un code pour s'assurer que c'est bien vous qui n'êtes pas forcément à la position B habituelle de connexion. (Exemple : autre réseau, localisation…).

Important :

Si vous activez la vérification en deux étapes, il vous faudra toujours deux formes d'identification. Si vous oubliez votre mot de passe, vous avez donc besoin de deux méthodes de contact. Ou si vous perdez votre méthode de contact, votre mot de passe seul ne vous permettra pas de vous reconnecter à votre compte.
Il peut s'écouler 30 jours pour que vous puissiez y accéder à nouveau.
Vous risquez même de perdre l'accès au compte.
Dans cette éventualité, nous vous recommandons vivement d'associer trois types d'informations de sécurité à votre compte.

Double authentification Google

Je préconise l'utilisation des services Google et application Google pour une double authentification sécurisée.

Pourquoi Google ?

C'est une référence numérique depuis de nombreuses année en termes d'utilisation globale à travers le monde en termes de recherche web et d'autres services.

Exemple :

Youtube, Maps, traduction, recherche, Android, Gmail (1,5 milliard d'utilisateurs dans le monde en 2018), Office 365, Play protect, Waze, Google Earth… et de très nombreux autres services utilisés à travers le monde.

Avec les années et les nombreuses mises à jour des services Google, la double authentification offerte par cette entreprise offre une sécurité conséquente et intuitive concernant les authentifications double et multi facteurs.

Configuration de Google Authenticator avec Google Play :

Configurer Google Authenticator

- Sur votre appareil, accédez à votre compte Google.
- En haut, dans le panneau de navigation, appuyez sur Sécurité.
- Sous "Se connecter à Google", appuyez sur Validation en deux étapes. Pour cela, vous devrez peut-être vous connecter.
- Dans la section "Ajouter d'autres deuxièmes étapes pour confirmer votre identité", sous "Application Google Authenticator", appuyez sur Configurer.
- Suivez les instructions à l'écran

Avantage du Google Authenticator :

Le google Authenticator bénéficie de plusieurs avantages pour les utilisateurs par sa simplicité et son efficacité. Exemple :

- En cas de perte de données (Vol, perte de téléphone, sinistre) l'utilisateur peut récupérer son compte auprès des services Google
- Logiciel évoluant régulièrement avec des mises à jour de sécurité.
- Google Authenticator peut générer des codes pour plusieurs comptes à partir d'un même appareil mobile. Une clé secrète distincte est nécessaire pour chaque compte Google.
- Transférer les codes Google Authenticator vers un nouveau téléphone
- Ajouter d'autres deuxièmes étapes pour confirmer votre identité.

  Configurez des étapes de secours supplémentaires pour pouvoir vous connecter même si les autres options que vous avez définies ne sont pas disponibles.
- Codes de secours. Ces codes imprimables à usage unique vous permettent de vous connecter lorsque vous n'avez pas votre téléphone sur vous, notamment lors de vos déplacements.
- Compatibilité du service avec des plateformes partenaires à Google (Facebook, Dropbox, Wordpress, IOS, Amazon…)
- Ajouter ou supprimer des appareils fiables.
- Extrême facilité d'utilisation.
- Pas besoin de connexion internet.