COMPUTERLAND
ERP & IT SERVICES

White Paper

Sécurisation de l'identité

Octobre 2022
Version : 1.2

1 Vue générale

1.1 Pourquoi sécuriser l'identité

Votre identité est précieuse et les hackers le savent. C'est pourquoi ils vont tenter par tous les moyens d'usurper celle-ci afin de pouvoir avoir accès aux ressources de votre entreprise afin de lancer des attaques.

Protéger l'identité de vos collaborateurs est une base fondamentale de la sécurité informatique.

Et en pratique, nous pouvons affirmer sans crainte qu'***une simple protection par mot de passe ne suffit plus*** : 80% des attaques ont pour origine un souci de mot de passe.

1.2 Azure Active Directory

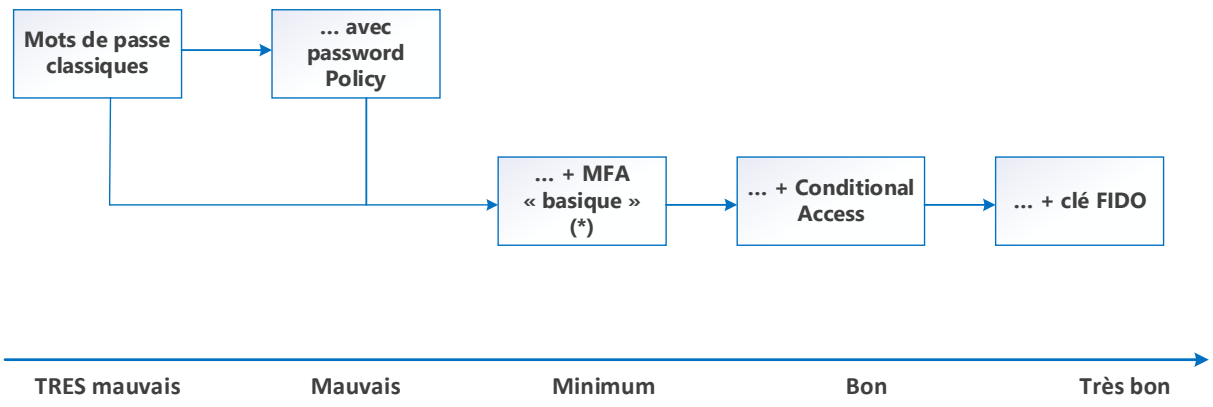
Pour les entreprises utilisant les technologies Microsoft, ***Azure AD doit idéalement être la source unique d'identification de l'entreprise***.

Ainsi, tout accès à une ressource de votre entreprise publiée sur internet, qu'elle soit localisée en interne, dans un cloud privé ou dans un cloud public devra passer par une authentification Azure AD ce qui garantit l'efficacité mais également un point unique de contrôle à surveiller et protéger.

1.3 Les différents modes de protection

Par ordre croissant de niveau de protection, nous résumons ci-dessous les différents niveaux de protection classiques à votre disposition.

Comme vous pouvez le constater, il est devenu indispensable d'avoir un mécanisme d'authentification multifacteur, autant que possible couplé à de l'accès conditionnel.



(*) comme indiqué au chapitre suivant, le MFA « basique » n'apporte un niveau de protection minimal que si le délai entre deux validations est abaissé de 90 jours à 7 jours au grand maximum.

2 Authentification multifacteur

2.1 Définition

L'authentification multifacteur (communément appelé MFA) ajoute une couche de protection au processus de connexion. Pour accéder à leurs comptes ou à des applications, les utilisateurs doivent confirmer leur identité par un mécanisme additionnel que nous détaillons ci-après.

Une bonne politique d'authentification multifacteur empêche 99,9% des attaques d'identité !

2.2 MFA basique

Les licences 365 d'entrée de gamme (Exchange Online, Business Standard, E1, …) permettent d'effectuer du MFA, mais uniquement de façon basique et sans aucune granularité.

C'est évidemment mieux qu'une simple protection par mot de passe, mais nous conseillons cependant à nos clients de rajouter la fonctionnalité de « Conditional Access » développée au chapitre suivant. Et ce pour les raisons suivantes :

- Le délai entre deux validations est de 90 jours (par défaut) ce qui n'est pas acceptable ;
- La gestion du MFA laisse à désirer et risque fort d'amener à des trous de sécurité ;
- La granularité est quasi inexistante (mode on/off) ;
- Il n'y a pas de prise en compte du type de matériel utilisé (dans le domaine ou « BYOD » – matériel personnel de l'utilisateur).

Si pour des raisons financières ce niveau minimum de sécurité devait néanmoins être utilisé, il est conseillé de configurer la demande de validation du MFA tous les 7 jours et de n'autoriser que le « mobile authenticator » de Microsoft ou une clé matérielle FIDO2 comme source de validation (voir chapitre « Méthodes d'authentification » ci-après.

2.3 Conditional Access avec MFA

Pré-requis : l'utilisation de règles d'accès conditionnels nécessite une licence Azure Active Directory P1 ou une suite comprenant celle-ci (M365 Business Premium, M365 E3, EMS E3, …).

Les différentes règles d'accès typiques à prendre en compte dans la mise en place sont les suivantes :

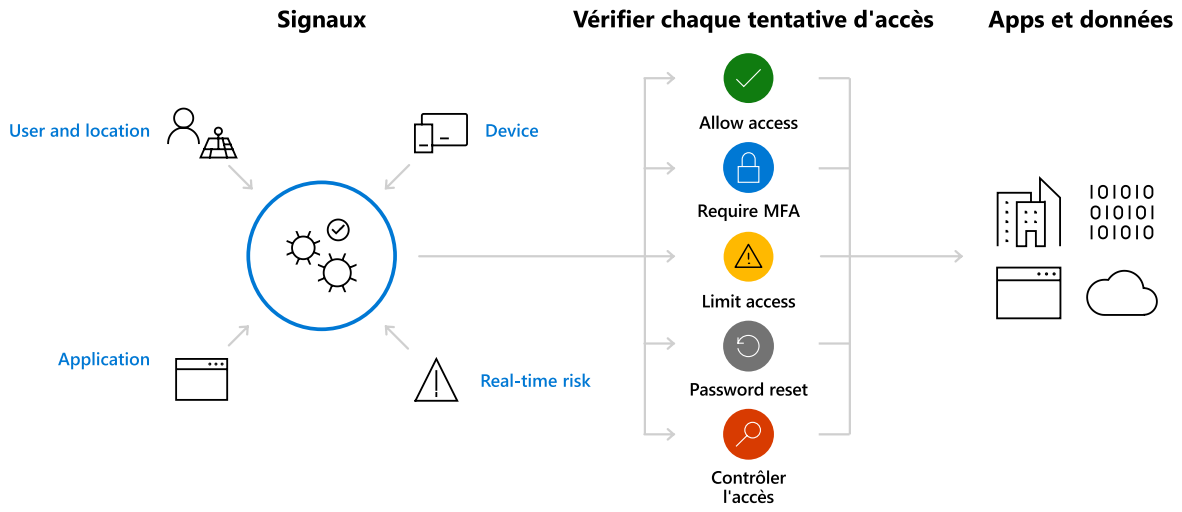
- **Géolocalisation** – il est important de permettre la géolocalisation des demandes MFA afin de refuser les demandes venant de pays où vos utilisateurs n'ont pas de raison d'être, ou de refuser des connexions venant de deux pays dans un délai matériellement trop court pour se rendre de l'un à l'autre. Des exceptions (temporaires ou non) peuvent être prévues.
- **Validation MFA**

  Pour cette partie notre recommandation est de créer 2 règles :
  - Demander la validation du MFA pour tous les utilisateurs disposant d'un rôle d'administration dans l'Azure AD avec une validité de 4 heures avant de devoir se réauthentifier ;
  - Demander la validation du MFA pour tous les autres utilisateurs avec une validité de 7 jours.

  Au niveau de ces règles, il est évidemment possible d'apporter des exceptions comme de ne pas devoir effectuer de validation du MFA quand la demande provient de l'IP publique du siège central.

- **<u>Blocage des plateformes non supportées</u>** / non utilisées – l'objectif étant ici de n'autoriser les accès que depuis Windows / IOS / Android ou MacOS en fonction de ce qui est réellement utilisé dans la société.
- Blocage des « legacy protocol » ;
- Blocage des machines n'étant pas en Hydride Azure AD Join ;
- Configurations nécessitant l'intégration avec la plateforme Intune :
  - Blocage des équipements ne répondant pas aux critères de sécurité (Compliance) ;
  - Limitation de l'accès aux applications approuvées ;
  - Limitation de l'accès sur base de Protection Policy.

Si des licences Azure Active Directory Plan 2 sont souscrites, il est alors possible d'ajouter la notion de gestion du risque, que ce soit au niveau de l'utilisateur ou de l'authentification.



2.4 Méthodes d'authentification MFA

Différentes méthodes existent afin de réaliser l'authentification multifacteur, nous les détaillons et comparons ci-dessous.

	Avantages	***Inconvénients***
Appel téléphonique	Très simple …	… mais **déconseillé** (trop de failles de sécurité)
Call / SMS sur smartphone	Très simple …	… mais **déconseillé** (trop de failles de sécurité)
App « MS Authenticator » sur smartphone	Simple	○ Nécessite une politique « BYOD » ○ Des failles de sécurité existent ○ Une « fatigue MFA » risque de s'installer (*)
Hello For Business	Aisé pour l'utilisateur	○ Uniquement pour les postes en Azure AD natifs ○ Pas valable pour smartphones
Clé FIDO2	Meilleur niveau de sécurité (**)	Coût un peu supérieur (45 € / clé)

L'authentification pas certificats numériques vient d'être ajoutée à cette liste, mais nous disposons à l'heure actuelle de trop peu de recul sur les tenants et aboutissants de celle-ci.

(*) en cas de trop nombreuses demandes d'authentification l'utilisateur est tenté (à la longue) de valider celles-ci de façon quasiment automatique.

(**) un compromis intéressant est de ne fournir une telle clé qu'aux utilisateurs disposant de droits d'administration ; ce sont en effet ceux dont la compromission de l'identité aura les conséquences les plus funestes.

2.5 En pratique

2.5.1 Mise en place

La durée de mise en place d'une politique de MFA avec Conditional Access dépendra des facteurs suivants :

- Du matériel BYOD (les utilisateurs sont autorisés à utiliser leur matériel personnels) est-il à prendre en compte ?
- La société dispose-t-elle d'une politique de mise à disposition de smartphones et/ou d'abonnement GSM ?
- Du home-working est-il autorisé ?
- Disposez-vous de plusieurs profils d'utilisateurs différents ((employés, ouvriers, …) ;
- La taille et la complexité informatique de la société.

Il faut typiquement compter entre 3 et 6 jours pour un projet de mise en place par un ingénieur système habilité.

2.5.2 Identity Management

Dans le domaine de la sécurité, il est illusoire de se croire en sécurité. La gestion de l'identité ne fait pas exception à la règle et une fois la politique MFA mise en place selon les règles de l'art, il est indispensable de régulièrement faire en sorte que le niveau de sécurité reste à un niveau acceptable.

C'est pourquoi, dans le cadre de notre contrat de maintenance c-Care, nous proposons maintenant un service « Identity Management » qui comprend les services proactifs suivants :

- Maintien de la configuration MFA ;
- Maintien de la « *baseline* » de Conditional accès pour accéder aux ressources de l'entreprise - telle que définie dans le projet de mise en place ;
- Maintien d'une géo-restriction adaptée à la société cible ;
- Analyse et suivi de l'utilisation des authentifications *legacy* & *oAuth 2.0* ;
- Externalisation des logs de connexion vers la solution Sentinel permettant de détecter un comportement inadéquat ;
- Vérification mensuelle du bon fonctionnement de l'outil Azure AD Connect ;
- Analyse trimestrielle du Secure Score du tenant et proposition de RFC pertinente ;
- Accès à un portail WEB permettant de lister les alertes de sécurité.