Microsoft

WAVESTONE

Sécurisation de l'Active Directory et d'Azure AD

Enjeux et trajectoires de transformation

Livre Blanc

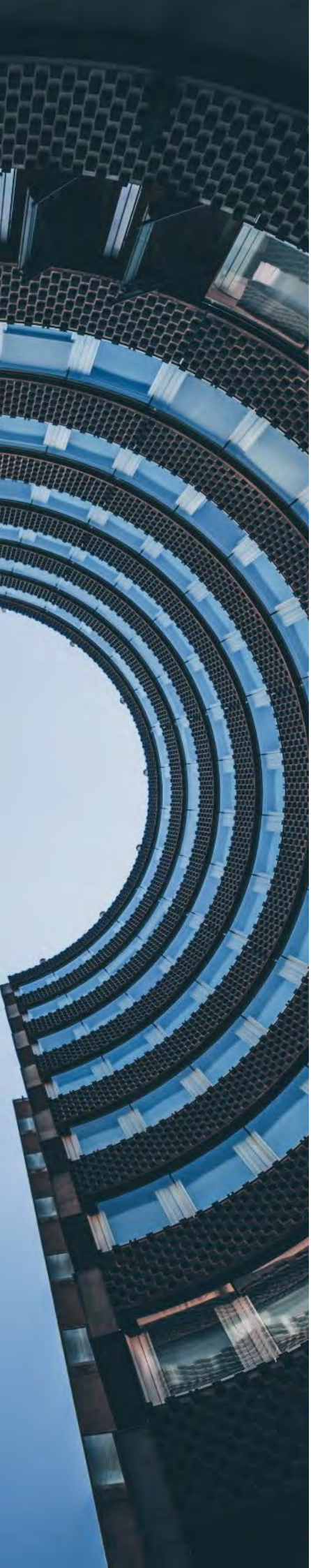
Introduction

Depuis plus de 20 ans qu'il existe, le service Active Directory est devenu un standard du marché, présent dans quasiment tous les systèmes d'information des organisations. Deux importantes tendances l'ont remis sur le devant de la scène ces dernières années.

La première découle de la forte exposition de ce composant à la menace cyber. S'agissant de la pierre angulaire du système d'information en matière de droits et de comptes à privilèges, l'Active Directory constitue une cible prioritaire pour les attaquants, qui cherchent à obtenir un accès large au système d'information en le compromettant. Ils peuvent ainsi l'utiliser pour déployer des logiciels malveillants ou encore pour accéder à des informations, avant de les faire fuiter. De vastes projets de remédiation ont ainsi été lancés ces dernières années, par de nombreuses organisations, pour y faire face.

La seconde découle de l'accroissement de l'usage de services collaboratifs, brusquement accéléré par l'explosion du recours au télétravail. Pour déverrouiller tous les nouveaux usages du modern workplace, la gestion des utilisateurs a étendu son champ d'action pour intégrer le périmètre dans le cloud, grâce à Azure AD. Dans la majorité des cas, il ne s'agit pas d'une bascule d'un tout on-premises vers un tout cloud, mais plutôt d'une extension de l'existant au travers d'architectures hybrides. Ce mouvement nécessite une prise en compte des enjeux de sécurité, pour ne pas exposer l'organisation.

Microsoft et Wavestone se sont associés pour analyser les tendances observées sur le terrain, lister les réflexions à mener et donner quelques clés et bonnes pratiques pour conduire les changements structurants.



Sommaire

Quelle est la maturité rencontrée sur le terrain ?

Ce chapitre vise à présenter le niveau actuel de sécurité rencontré pour l'Active Directory et Azure AD.

Nous reviendrons dans un premier temps sur les grands types d'architecture rencontrés et les enjeux de sécurité, puis nous partagerons les enseignements tirés des attaques rencontrées par le CERT Wavestone (CERT-W).

Quelles architectures et quel bilan de la maturité cybersécurité ?

Trois grands types d'architecture peuvent être rencontrées :

Architecture AD *on-premises*

Architecture historique de moins en moins rencontrée chez les clients (<10%). Il s'agit généralement de clients ayant des enjeux forts de souveraineté.

Architecture hybride AD/Azure AD

Cette architecture tirée par l'essor d'Office 365 est aujourd'hui majoritaire chez les clients (80 à 95%). Des variations d'implémentation existent cependant, en particulier sur la synchronisation ou non des hashs de hashs des mots de passe.

« Seules 25% des authentifications sont encore réalisées on-premises »

Architecture 100% Azure AD

Présente uniquement pour de nouvelles entités construites avec un prisme 100% numérique (<5%). Elle nécessite d'avoir un système d'information qui répond à un certain nombre de prérequis.

Active Directory *on-premises* ou le poids de l'histoire

L'Active Directory est organisé autour de domaines regroupés en une ou plusieurs forêts. Il n'est pas rare, pour des grandes organisations, d'avoir plus de 100 domaines ou forêts.

Cette architecture complexe s'explique par le poids de l'histoire et les multiples transformations subies par l'entreprise : fusions, acquisitions, réorganisations, etc.

L'Active Directory n'étant pas vu comme une application « apportant de la valeur au métier », l'intégration des nouveaux périmètres a été réalisée en minimisant les évolutions (moyen le moins cher et le plus rapide), sans réflexion globale sur l'optimisation de l'architecture. Des relations de confiance entre domaines ou forêts ont été ajoutées, pour permettre à un utilisateur d'être reconnu partout dans le SI.

Un faible niveau de sécurité

Dans la majorité des organisations, le maintien en condition de sécurité de l'AD passe souvent uniquement par l'application des correctifs de sécurité et le traitement de l'obsolescence de l'OS.

« Le SI est compromis en moins de 24h dans 80% des audits réalisés »

Wavestone, audits AD 2020

Les mises à jour fonctionnelles sont quant à elles peu mises en œuvre, généralement par méconnaissance ou par crainte des impacts possibles suite à l'extension du schéma. Les organisations ne profitent donc pas des nouvelles fonctionnalités, permettant de limiter les risques de sécurité (par exemple la mise en œuvre du groupe *protected users, Authentication Silos* et *Kerberos Armoring*). De la même façon, trop rares sont les organisations à désactiver les protocoles obsolètes.

Il n'est pas rare d'avoir des organisations avec des centaines de comptes Administrateurs de domaine ou d'entreprise alors que les bonnes pratiques et l'application du principe de moindre privilège signifieraient de les limiter à moins de 5. Cette situation s'explique par la difficulté à assurer la conduite du changement (retirer des droits peut être vu comme une rétrogradation ou une dépossession). Mais aussi la demande de comptes de services avec des droits excessifs pour faciliter l'intégration d'une nouvelle application.

Les évolutions de l'architecture, en particulier la mise en œuvre de relations de confiance, ont été définies uniquement sous le prisme fonctionnel sans évaluer les risques de propagation d'une attaque entre les domaines et les forêts. Wavestone rencontre régulièrement pendant des audits un domaine abandonné avec une relation de confiance bidirectionnelle. Et c'est bien lui qui définit le niveau global de sécurité !
De la même façon, la mise en œuvre d'Azure AD a visé à répondre à des besoins fonctionnels sans considération de sécurité. Rares sont les organisations à avoir défini un processus de gestion des comptes à privilèges adapté aux particularités d'Azure AD. Autre exemple, seuls 30%(*) des comptes administrateur général (ou Global Administrator) ont l'authentification multi-facteur (MFA) activée, alors que la fonctionnalité est native et gratuite.
(*) Microsoft août 2021

Une prise de conscience récente des enjeux de sécurité

Dans le contexte actuel d'explosion des attaques exploitant des défauts de configuration de l'AD, il n'est plus rare de voir le COMEX interroger le DSI ou le RSSI sur le niveau de sécurité de l'AD et valider des enveloppes de plusieurs centaines de milliers voire millions d'euros pour mener des projets de refonte et de sécurisation.

« 53% des grandes entreprises ont un projet de sécurisation de l'AD »
Baromètre CESIN 2021

Les projets de sécurisation de l'AD sont lancés pour la vaste majorité mais les audits menés par Wavestone, nous montrent que :

> *« Moins de 10% des clients ont correctement implémenté les bonnes pratiques de sécurité »*
> Wavestone, audit AD 2020

En effet, bien que les pratiques d'administration aient pu évoluer, il reste bien souvent des défauts de configuration qui permettent de remonter au Tier 0 (concept détaillé dans le chapitre 2). Des chemins de compromission et d'élévation de privilèges peuvent par exemple se cacher dans des droits d'accès (ACL) dangereuses configurées sur les objets du Tier 0, ou subsister du fait de mauvais usages des comptes à hauts privilèges. Le modèle de sécurité AD est détaillé au chapitre 2..

Une architecture 100% Azure AD, la cible pour tous ?

Aucune grande organisation n'est aujourd'hui en mesure de remplacer totalement son AD on-premises par un service 100% porté par l'Azure AD. Peu d'organisations sont en mesure d'avoir un SI qui remplisse l'ensemble des prérequis technologiques pour faire cette transformation (postes de travail gérés avec un MDM (Mobile Device Management) et Azure AD, absence d'applications utilisant une authentification NTLM *(NT Lan Manager)*, Kerberos ou LDAP (*Lightweight Directory Access Protocol)*, création des utilisateurs dans le cloud, etc.). L'usage d'un service d'AD managé pourrait être une option pour assurer la rétrocompatibilité sans avoir à gérer le Tier 0.

L'usage du cloud peut être vu comme une délégation à Microsoft de la maitrise des risques, mais elle n'est que partielle. Les clients restent responsables de la configuration de la plateforme, des identités et des données. Malheureusement la prise de conscience reste faible. Pour rappel, un nouvel abonnement à la solution Teams s'accompagne de la création d'une souscription Azure AD.

32/100

Secure score moyen

34,6 score le plus élevé pour le secteur technologie

24 score à la création d'une souscription Office 365 E3

Il est important que les organisations prennent possession des outils proposés pour piloter leur sécurité et qui n'existaient pas on-premises (ils peuvent néanmoins nécessiter des niveaux de licence avancés). Le Secure Score (détaillé dans un focus ci-après) - cible visé par les organisations - devrait être au minimum entre 60 et 70.

FOCUS

Azure AD : un annuaire *cloud*

Azure Active Directory (Azure AD), lancé en novembre 2011, est une solution d'Identity as a Service (IDaaS).

Azure AD, fournit aux organisations les fonctionnalités pour gérer l'authentification des applications modernes (SAML et WS-Federation, OAuth2, OpenID Connect et FIDO2).

Il ne s'agit pas d'Active Directory dans le Cloud mais bien d'une nouvelle solution.

Azure AD a été conçue sur une architecture cloud, basée sur des micro-services, répartie sur plusieurs zones géographiques.

Un tenant Azure AD est automatiquement créé lorsqu'une organisation souscrit à un service cloud de Microsoft, tel qu'Azure ou bien Office 365.

Graph API

Pour interroger et mettre à jour les objets de l'annuaire, Azure AD propose une *Application Programming Interface* (API) qui se nomme Graph API.

Graph API est une passerelle unifiant de nombreuses autres API REST telles que celles d'Exchange Online, OneDrive, Endpoint Manager ou bien Security Graph.

Un remède miracle?

Bien que la majorité des attaques courantes cible aujourd'hui l'AD, une migration vers Azure AD n'est pas pour autant un remède miracle. Azure AD simplifie la mise en œuvre de l'authentification forte sans mot de passe ou bien le contrôle d'accès conditionnel basé sur les risques, cependant les comptes à privilèges doivent toujours être fortement encadrés.

Il est impératif de mener à bien un projet de sécurisation pour maitriser cette nouvelle brique et profiter de la transformation pour passer à des pratiques d'administration à l'état de l'art.

En particulier, il est recommandé :
/ D'auditer la configuration d'Azure AD, de valider régulièrement les membres des rôles privilégiés ainsi que les applications autorisées à interagir avec Azure AD ;
/ De développer des scénarios de détection spécifiques pour limiter le temps pendant lequel les intrus demeurent invisibles dans le SI.

345 Millions

Azure AD gère plus de 345 millions d'utilisateurs actifs chaque mois, avec une moyenne de 30 milliards de demandes d'authentification par jour.

FOCUS

NTLM, toujours le talon d'Achille de la sécurité ?

NTLM (NT LAN Manager) est utilisé par les applications pour authentifier les utilisateurs et, éventuellement, pour fournir une sécurité de session lorsque l'application le demande.

Les protocoles NTLM sont des protocoles d'authentification obsolètes qui utilisent une méthode de défi et réponse pour que les clients puissent prouver mathématiquement qu'ils possèdent le condensat de mot de passe, le *hash* NT. Les versions actuelles et passées de Windows prennent en charge plusieurs versions de ce protocole, dont NTLMv2, NTLM ainsi que le protocole LM.

Depuis Windows 2000, le protocole Kerberos est le protocole d'authentification par défaut. Cependant, si le protocole Kerberos n'est pas négocié pour une raison quelconque, alors les applications reliées à Active Directory tenteront d'utiliser un des protocoles NTLM, si disponible.

Toutes les versions de NTLM sont vulnérables à des attaques largement documentées. Pour cette raison, le protocole NTLM n'est pas supporté dans Azure Active Directory, peut être désactivé dans Azure AD DS ainsi que dans Active Directory.

Au-delà d'un support cryptographique faible, l'absence d'authentification du serveur peut permettre à un attaquant d'usurper l'identité d'un serveur. Ainsi, les applications utilisant NTLM peuvent être vulnérables à une attaque par « réflexion » : un attaquant peut détourner l'échange d'authentification d'un utilisateur vers un serveur légitime et l'utiliser pour s'authentifier sur un autre ordinateur, voire sur l'ordinateur de l'utilisateur.

> Le protocole NTLM n'est pas supporté dans Azure Active Directory.

La suppression complète de NTLM dans un environnement améliore indéniablement la sécurité en éliminant les attaques de type PtH (*Pass-The-Hash*). Cependant, cela ne permet pas d'éliminer d'autres classes d'attaques, comme le vol de mots de passe en clair ou bien le vol de tickets Kerberos, *Ticket Granting Ticket* (TGT).

Les organisations sont encouragées à mettre en œuvre Kerberos ou à utiliser des protocoles d'authentification modernes (OpenID Connect, SAML, etc.) pour leurs applications existantes, car Microsoft ne prévoit aucune amélioration du protocole NTLM.

Pourquoi NTLM est-il toujours utilisé ?

NTLM est encore largement utilisé du fait d'applications historiques qui n'ont pas évolué, mais aussi en raison de mauvaises configurations d'applications qui supportent pourtant Kerberos.

FOCUS

En finir avec NTLM – 4 étapes

1 – Identifier tous les cas d'utilisation de NTLM

Recenser les appareils et les applications liés à NTLM, les classifier et déterminer ce qui devra potentiellement être traité dans une stratégie d'exception.

2 – Préparer les applications à utiliser le package Negociate

Résoudre les problèmes de compatibilité (dont le remplacement de matériels et de logiciels), configurer les applications pour utiliser le package de sécurité Negociate pour laisser l'OS utiliser le meilleur protocole d'authentification disponible et mettre en œuvre les prérequis (Kerberos ou autres)

3 – Activer le blocage global de NTLM avec une stratégie d'exception

Bloquer l'utilisation de NTLM sauf pour les applications et matériels qui ne peuvent pas évoluer et qui devront être traités dans une stratégie d'exception (étape 4).

4 – Isoler les applications ne pouvant évoluer et durcir la configuration de NTLM

Isoler les appareils et les applications avec une logique de segmentation réseau. Durcir la configuration de NTLM et superviser les authentifications en continue.

Il est déconseillé de bloquer sans discernement l'utilisation de NTLM, sans avoir au préalable cartographié les applications existantes et conduit une analyse d'impact.

Retour d'expérience sur des attaques rencontrées par le CERT-W

L'AD, au cœur de la menace rançongiciel et du mode opératoire des attaquants

Au cœur de la sécurité des systèmes d'information, l'AD est aujourd'hui la cible privilégiée des attaquants lors d'attaques informatiques d'envergure.
Le benchmark 2020 du CERT Wavestone est sans équivoque.

> *« L'AD a été compromis dans 95% des crises cyber traitées par le CERT-W »*

Ce constat est par ailleurs partagé par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI): *L'analyse des modes opératoires des attaques récentes met en évidence une recrudescence du ciblage des annuaires Active Directory*. Ce constat s'explique par le rôle central joué par l'AD au sein des SI d'entreprise.
L'obtention de privilèges AD élevés permet bien souvent à un attaquant de prendre le contrôle de l'ensemble de l'écosystème Windows, voire de rebondir sur d'autres environnements au travers des postes de travail de développeurs et d'administrateurs. Suite à cette compromission, des données sensibles peuvent être exfiltrées ou les activités et services métiers perturbés durablement, au travers d'attaques par rançongiciels notamment.
Les années 2019 et 2020 ont de fait été marquées par un accroissement sans précédent des attaques par rançongiciel.

La grande majorité des interventions de crise du CERT-W sur l'année 2020, tous secteurs confondus, visait à répondre à des déploiements de rançongiciels.

192

Le nombre d'attaques par rançongiciels affectant le territoire national portées à la connaissance de l'ANSSI en 2020, en hausse de 255% par rapport à 2019.

Constat partagé par l'équipe de réponse à incidents Microsoft *(Detection and Response Team ou DART).*
Fait relativement récent, une part importante des demandes de paiement de rançons est aujourd'hui doublement axée sur la restauration des données chiffrées et la non-divulgation de données exfiltrées. Cette combinaison de blocage du SI et de la fuite de données s'est développée progressivement du fait des actions du groupe Maze en Amérique du Nord.

Les possibilités d'exécution de code distribué offertes par l'AD, comme les stratégies de groupe (GPO) ou les droits d'administration locaux sur les machines jointes à l'AD, sont exploitées par les attaquants pour déployer les charges entraînant le chiffrement des systèmes. Parfois employées simultanément, les GPO et les accès directs aux systèmes via des outils d'administration légitimes, permettent un chiffrement de l'ensemble du parc Windows en l'espace de quelques heures.

Les sauvegardes sont-elles à l'abri des attaquants ?

S'il est encore rare que les infrastructures de sauvegarde soient ciblées spécifiquement, elles peuvent faire partie des dommages collatéraux des attaques. En l'absence d'une infrastructure de sauvegarde dédiée et non intégrée à la forêt AD de production, le déploiement de la charge chiffrante à l'échelle du parc entraîne un chiffrement des systèmes de sauvegarde.

Uniquement pour une minorité des attaques investiguées par le CERT-W, les groupes d'attaquants ont explicitement ciblé les sauvegardes, que ce soit au niveau des socles systèmes des serveurs de sauvegarde ou au travers des consoles d'administration implémentant une authentification unique avec l'AD.

Cette tendance, permettant de maximiser les chances de paiement de la rançon, devrait s'accentuer dans les mois et années à venir.

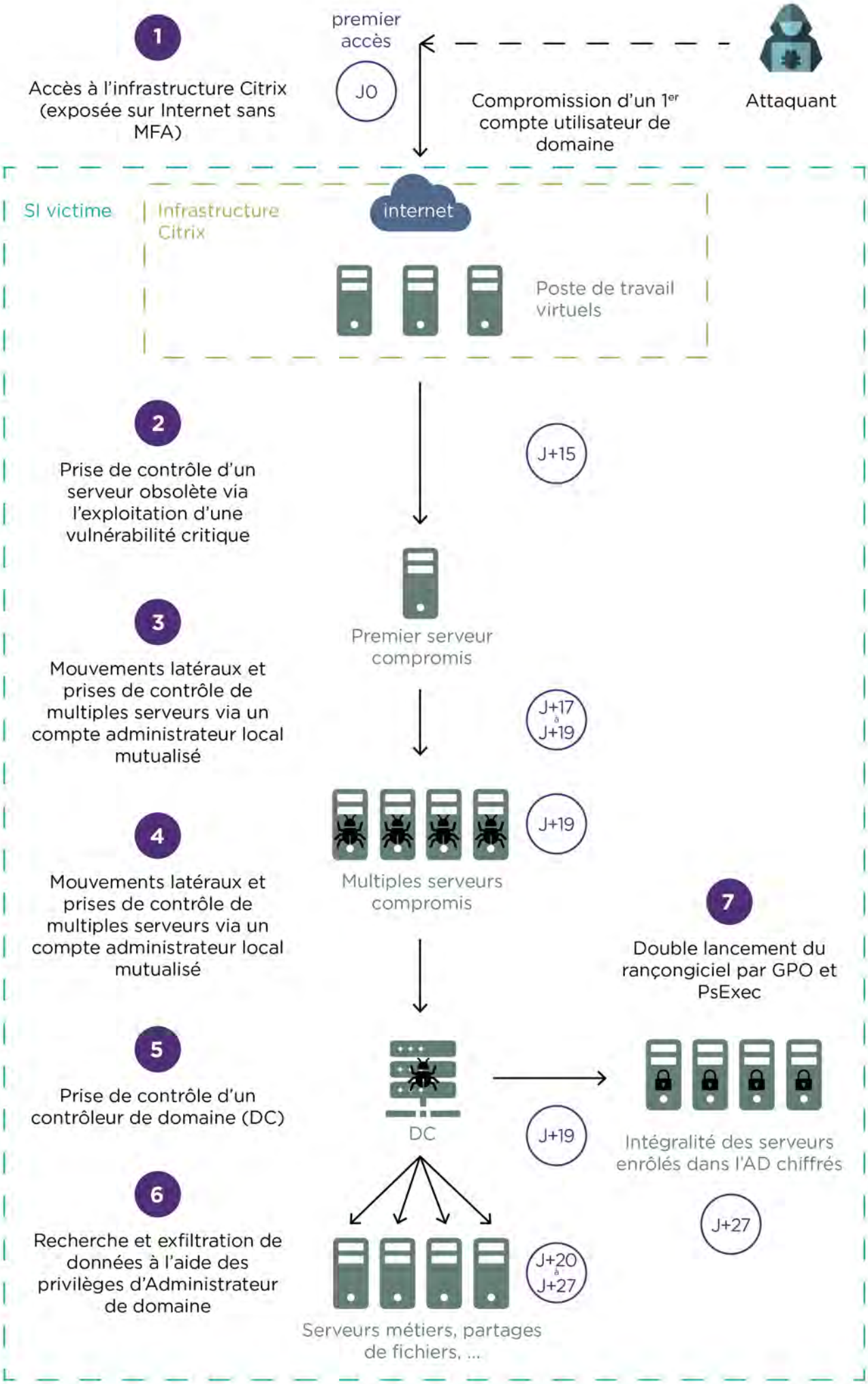
Étude d'une attaque par rançongiciel, basée sur une intervention du CERT-W en 2020

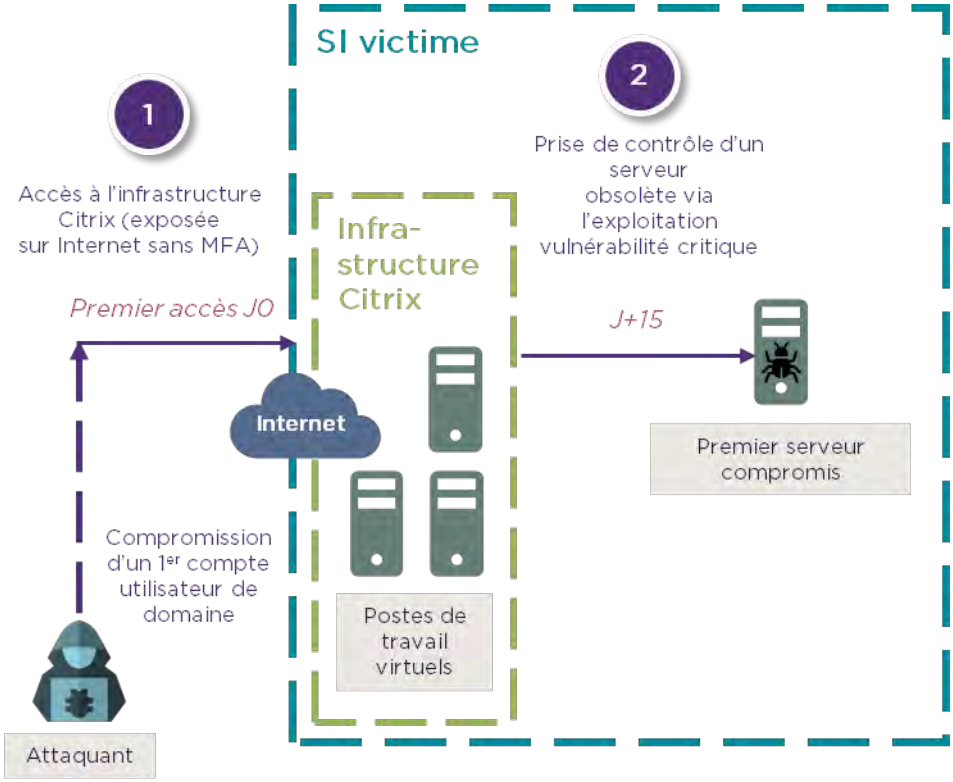
L'attaque présentée est inspirée d'une intervention du CERT-W faisant suite au déploiement d'un rançongiciel sur un parc de plusieurs dizaines de milliers de machines. Présentant les vulnérabilités et défauts de configuration communément exploités, l'analyse met en lumière les *Tactics, Techniques and Procedures* (TTP) d'un opérateur de rançongiciel. Toutes les informations permettant d'identifier les parties ont été anonymisées.

Les élévations de privilèges au sein des environnements Active Directory, suite à la compromission initiale d'une première ressource, font ainsi partie intégrante des modes opératoires des groupes d'attaquants. Une absence de techniques d'attaques avancées est constatée dans la majorité des attaques par rançongiciels, et notamment dans le cadre d'attaques selon le modèle du *Ransomware-as-a-Service*. Dans ce modèle, des cybercriminels sont affiliés à un fournisseur de rançongiciel, afin de bénéficier de l'agent chiffrant et des services liés (infrastructure de paiement et de contact, site de publications, etc.) en échange d'une part des gains des opérations. Les groupes d'attaquants agissent ainsi principalement sur opportunité et avec des objectifs de retour sur investissement à court terme. Au moins une des phases de la chaîne d'attaque aurait en général pu être évitée au travers d'un meilleur respect des bonnes pratiques de base en matière de cyber-hygiène et de sécurité informatique.

Au-delà des attaques non ciblées et opportunistes, des groupes d'attaquants par rançongiciels font toutefois usage de moyens et compétences plus avancés dans la réalisation de leurs opérations. Cette tendance, dénommée « *Big Game Hunting* », permet aux groupes cybercriminels de cibler des organisations disposant d'un niveau de sécurité informatique plus élevé.

Schéma de principe de l'attaque étudiée





Accès initial

L'attaquant s'introduit sur le SI, suite à la compromission initiale d'un compte de domaine, via une infrastructure de bureaux virtuels exposée sur Internet. Une réutilisation des identifiants compromis est de fait possible en l'absence d'authentification multi-facteurs.

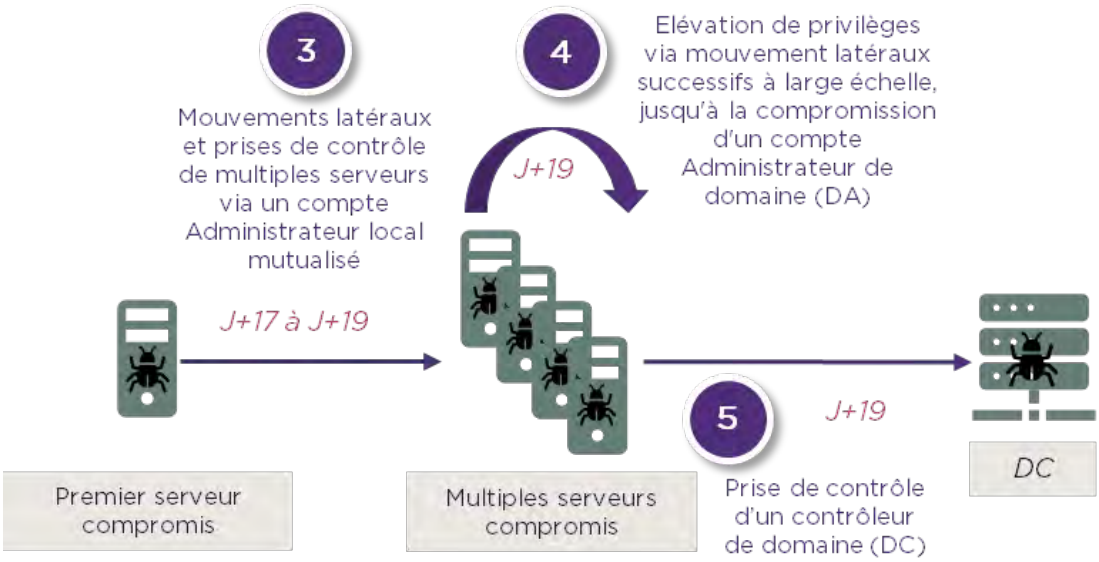
L'exposition de service d'accès sur Internet sans MFA expose le SI à des accès illégitimes par rejeux d'identifiants

Si le hameçonnage et l'exploitation de vulnérabilités critiques se maintiennent comme les principaux vecteurs d'infection, les rejeux d'identifiants sur des services d'accès distants exposés sans authentification multi-facteurs représentent près de 1 cas sur 5 des compromissions initiales investiguées par le CERT-W. On peut notamment citer le cas des attaques par force brute sur les services *Remote Desktop Protocol* (RDP) exposés sur Internet.

Suite à cet accès, un échappement du bureau restreint (via un interpréteur de commandes exécuté au travers d'un logiciel autorisé) permet à l'attaquant d'obtenir un accès au système et d'entamer une phase de reconnaissance active. Fait courant, un délai a été constaté entre le premier accès malveillant et le début de la phase de reconnaissance active. Ce délai peut s'expliquer par la revente de l'accès, obtenu par un groupe d'attaquants spécialisés dans le domaine, à l'opérateur de rançongiciel.

L'exploitation d'une vulnérabilité critique sur un serveur Windows 2003 (en fin de support et ne recevant plus de correctifs de sécurité) permet à l'attaquant de prendre le contrôle du serveur à distance et d'établir un camp de base sur le serveur.

L'absence de déploiement de la solution LAPS[1] facilite les mouvements latéraux



Latéralisation et élévation de privilèges

Des rebonds depuis le serveur compromis à l'aide du compte administrateur local, dont le mot de passe est mutualisé avec les comptes de multiples autres serveurs, permettent ensuite à l'attaquant d'élever ses privilèges.

Les serveurs obsolètes doivent être isolés et ne pas dégrader le niveau de sécurité de l'ensemble du SI

Un premier compte de domaine privilégié est ainsi compromis puis des tentatives de mouvements latéraux à large échelle sur plusieurs milliers de machines sont réalisés avec ce compte jusqu'à la compromission d'un compte administrateur de domaine.

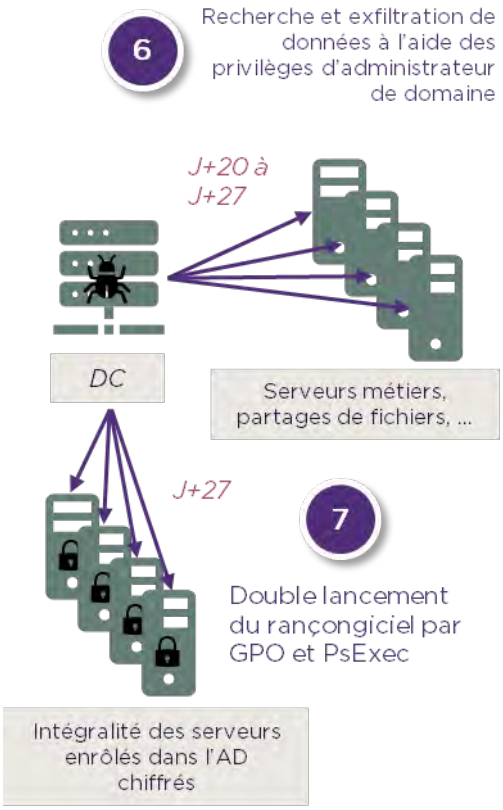
1. La solution logicielle Microsoft LAPS (Local Administrator Password Solution) fournit une capacité de gestion automatisée des mots de passe des comptes locaux des machines intégrées à l'AD et permet de garantir l'unicité du mot de passe d'un compte local par machine.

Bien qu'une solution antivirale (par signatures) était déployée sur les systèmes ciblés, des utilitaires présents nativement sur les systèmes Windows permettent d'exfiltrer la mémoire du processus LSASS (qui contient les secrets d'authentification des utilisateurs connectés).

L'usage de comptes disposant des privilèges d'administrateur du domaine pour des tâches courantes rend possible une élévation de privilèges via des mouvements latéraux successifs.

L'absence de mise en œuvre d'une administration structurée par niveau (modèle de tiering) expose le domaine AD à des élévations de privilèges

Suite à la compromission du domaine, une phase de post-exploitation est entamée par l'attaquant, dans le but d'identifier et exfiltrer les données sensibles de l'entreprise. Les privilèges d'administrateur du domaine permettent ainsi un accès très large aux ressources enrôlées (partages de fichiers réseau, boîtes de messageries, etc.).



Déploiement du rançongiciel

En dernière étape, la charge malveillante est déployée à la fois par stratégie de groupe et un processus automatique, exécuté depuis un contrôleur de domaine, pour permettre une rapide propagation au sein du SI de la victime.

En sus du chiffrement des machines compromises, l'agent chiffrant efface les journaux de Windows hébergés sur les machines et les éventuelles copies conservées localement.

Une tendance émergente : les attaques par supply-chain

Au-delà des vecteurs de compromission plus communs, les attaques dites par *supply-chain* représentent un vecteur d'infection en croissance. Bien que documentées depuis plusieurs années déjà, les attaques réalisées via des fournisseurs et prestataires de services se sont multipliées, en nombre et en ampleur ces deux dernières années. Cette croissance peut notamment s'expliquer par l'amélioration du niveau de sécurité informatique des infrastructures d'entreprise, obligeant ainsi les attaquants à compromettre des tiers pour atteindre leurs cibles finales.

Les privilèges accordés sur l'annuaire AD aux solutions tierces, souvent requis trop élevés par les éditeurs par soucis de simplicité, peuvent se révéler désastreux en cas d'attaque par supply-chain.

Les attaques par *supply-chain* présentent de plus un retour sur investissement particulièrement attractif pour les groupes d'attaquants : la compromission d'une première entité mène potentiellement à l'obtention d'un point d'accès chez un grand nombre de ses clients. Réservées aux attaquants dotés de capacités techniques les plus avancées, ces attaques ont aussi bien été employées par les opérateurs de rançongiciels, à des fins de gains financiers, que par les groupes étatiques, dans une optique d'espionnage.

En 2020, l'attaque SolarWinds a marqué les esprits. Cette attaque démontre l'ampleur que peuvent prendre les attaques par *supply-chain*, avec 18 000 des clients de SolarWinds impactés. Très sophistiquée dans son mode opératoire d'intrusion (injection d'une charge à la compilation, déploiement d'infrastructures dédiées pour chaque cible finale, etc.), cette attaque fait aussi état de techniques de latéralisation classiques et repose, en partie, sur des vulnérabilités ordinaires.

L'attaquant a créé très rapidement des portes dérobées, a ouvert discrètement des canaux de communication, a camouflé et caché ses traces alors qu'il cherchait des moyens d'obtenir des privilèges élevés. Mais il a également utilisé des techniques connues telles que la réutilisation de mots de passe compromis ou le déplacement latéral avec des comptes administrateurs identiques sur l'ensemble de machines.

Quelles trajectoires pour améliorer la situation ?

Ce chapitre vise à expliquer le nouveau modèle de sécurité AD *Enterprise Access Model* puis à proposer des recommandations de sécurisation pour l'AD *on-premises* et Azure AD, ainsi qu'une trajectoire pour une modernisation vers Azure AD.

Enterprise Access Model

Microsoft a introduit en 2012, le modèle d'administration en tiers dont l'objectif est de partitionner les secrets d'authentification au sein d'un environnement Active Directory.

Le principe d'implémentation est de créer un cloisonnement entre les administrateurs en fonction des ressources qu'ils gèrent. Cela aide à protéger les secrets d'authentification et éviter qu'une compromission d'un niveau de moindre confiance ne se propage à un niveau de plus grande confiance.

Ce concept se fonde sur le modèle de Bell LaPadula, introduit dans les années 1970.

Ce modèle définit trois niveaux pour séparer l'administration des ressources en fonction de leur criticité. Ainsi, les administrateurs qui contrôlent les postes de travail des utilisateurs sont séparés de ceux qui gèrent les serveurs et de ceux qui gèrent le référentiel d'identités de l'entreprise, ici l'Active Directory. Les documents Mitigating Pass-the-Hash and Other Credential Theft, version 1 and 2 détaillent ce modèle d'administration associé à un Environnement d'administration à sécurité renforcée (*Enhanced Security Admin Environment* - ESAE) communément appelé « forêt d'administration » ou bien encore « *hardened forest* ».

En décembre 2020, Microsoft à fait évoluer ce modèle d'administration pour prendre en compte les environnements *cloud* et hybride. Ce nouveau modèle d'accès entreprise (*Enterprise Access Model*) est une évolution du précédent modèle : le concept de modèle en tiers demeure, bien qu'il soit remanié avec une terminologie qui évolue.

L'approche ESAE a été supprimée des recommandations générales, car complexe et coûteuse à implémenter. La mise en œuvre d'une forêt d'administration peut néanmoins rester pertinente dans certains cas, notamment pour les environnements déconnectés.

Comprendre le modèle précédent, en tiers

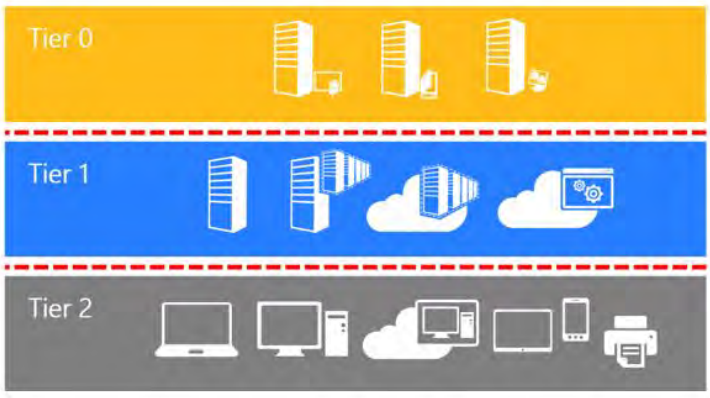
Comprendre les principes du modèle de *tiering* est fondamental pour bien appréhender les bonnes pratiques de sécurité dans un environnement Microsoft.

Des moyens techniques sont appliqués pour assurer l'isolation entre les tiers.

Le Tier 0 est le niveau le plus privilégié et comprend les comptes, les groupes, les contrôleurs de domaine et les ressources qui ont contrôle direct ou indirect sur Active Directory. On placera donc dans ce niveau 0, les serveurs liés à l'Active Directory (contrôleurs de domaine) mais également les autres composants ayant une interaction forte tels que les serveurs de fédération, serveurs de mises à jour WSUS, de déploiement des applications, PKI interne, ou bien encore Azure AD Connect.

Les administrateurs du Tier 0 peuvent gérer et contrôler les ressources de tous les niveaux (au sens AD), mais ne doivent interagir qu'avec les ressources du Tier 0. Pour ce faire, ils doivent utiliser une station d'administration à sécurité renforcée (appartenant à ce niveau).

Le Tier 1 désigne les serveurs et les applications qui sont membres du domaine AD ainsi que les ressources qui gravitent autour. Les comptes qui contrôlent ces ressources ont potentiellement accès à des données sensibles. Les administrateurs de niveau 1 peuvent accéder aux ressources du Tier 1 et ne peuvent gérer dans l'Active Directory que les ressources du Tier 1.



Le Tier 2 concerne les appareils des utilisateurs (postes de travail, imprimantes, etc.). Par exemple, le support téléphonique (le service d'assistance, fait partie de ce niveau). Les administrateurs du Tier 2 ne peuvent se connecter qu'aux ressources du Tier 2 et ne gérer que les actifs du Tier 2 dans l'annuaire Active Directory.

Un nouveau modèle pour l'entreprise hybride

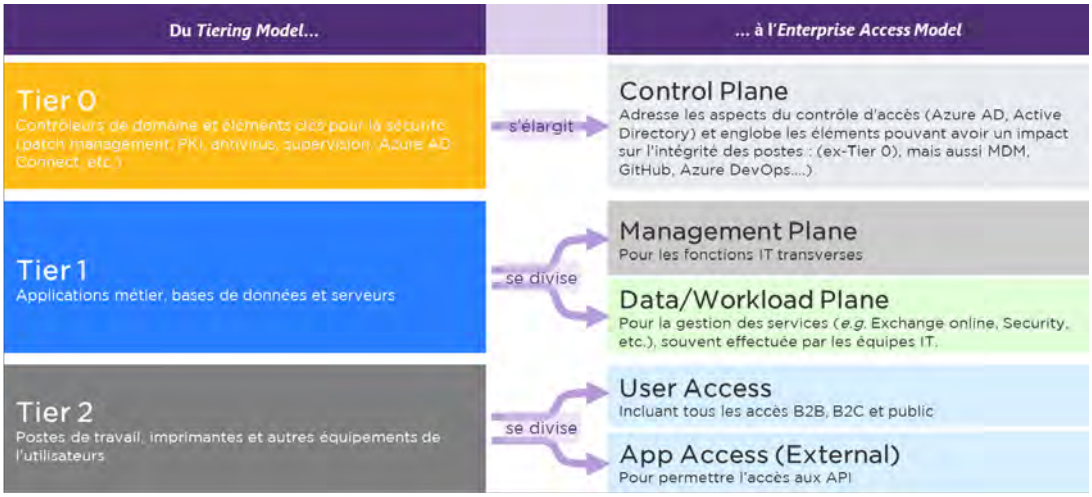
Le nouveau modèle d'accès d'entreprise (Enterprise Access Model) a été créé pour les organisations hybrides, qui ont des applications *on-premises* mais également *multi-cloud* suivant les principes de sécurité du *Zero Trust*.

Dans ce nouveau modèle, le contrôle de la sécurité n'est plus opéré exclusivement à partir d'Active Directory, mais également depuis Azure Active Directory.

Les termes évoluent mais les principes de séparation en niveaux de privilèges (*tiering*) demeurent.
Ainsi, on ne parle plus de Tier 0, mais de plan de contrôle (*Control Plane*). La gestion du plan de contrôle doit être étroitement encadrée et limitée à des appareils de très forte confiance. Le plan de contrôle évolue et s'élargit : au-delà des ressources de l'ancien Tier 0, on y ajoute Azure AD, mais aussi les solutions *cloud* comme les outils de gestion d'appareils de type MDM ou bien les solutions de développement comme GitHub/Azure DevOps.

La notion des couches de gestion est introduite à travers le *management plane* et le *data/workload plane* qui sont là pour gérer les applications et les données, ce qui s'appelait auparavant le Tier 1. Enfin, il y a les utilisateurs et les autres applications qui consomment les services (applications et données) – il peut s'agir d'utilisateurs internes, de partenaires, de clients, etc.

L'*Enterprise Access Model* ne mentionne pas explicitement les postes de travail des utilisateurs qui étaient situés auparavant dans le Tier 2. À la place, le plan de contrôle d'Azure AD est utilisé pour déterminer quels types d'appareils peuvent se connecter à tel service ou application. C'est ce qui se nomme le contrôle d'accès conditionnel et constitue la pierre angulaire d'une architecture dite *Zero Trust*.



Securing Privileged Access « mode d'emploi »

Au travers du guide Securing Privileged Access, Microsoft a partagé une implémentation de référence qui illustre le modèle d'accès entreprise introduit précédemment.

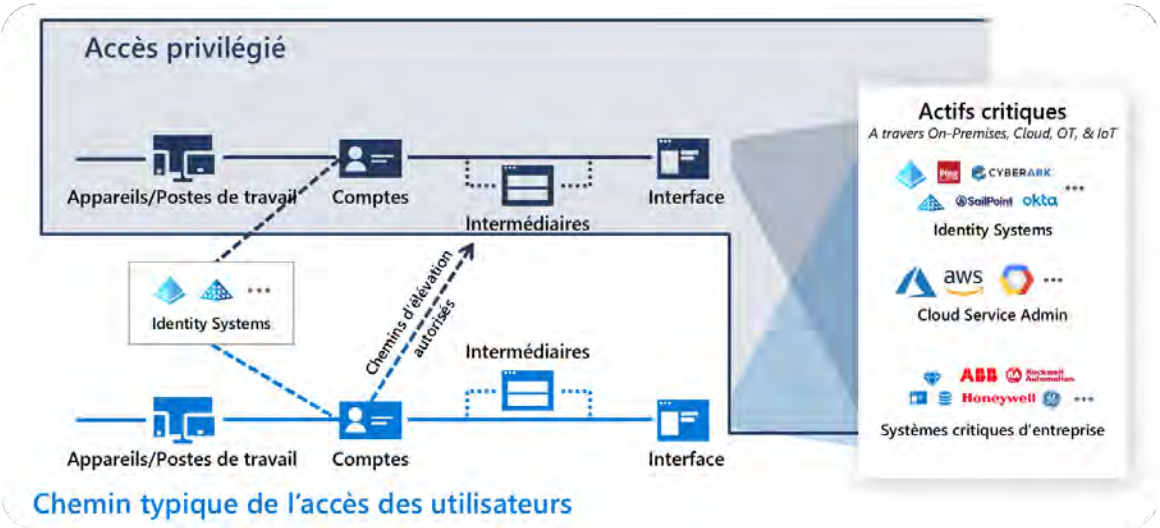
L'objectif est de limiter strictement la capacité à effectuer des actions privilégiées sur des chemins autorisés, tout en perturbant le retour sur investissement des attaquants.

Au-delà de la prévention, on surveille de près ces chemins d'accès en détectant les anomalies et les comportements déviants.

La stratégie est d'encourager les organisations à d'abord utiliser les nombreuses fonctionnalités nativement présente dans le *cloud*.

Dans le guide proposé par Microsoft, l'implémentation s'appuie sur les solutions de sécurité disponibles dans Microsoft 365 Entreprise E5. C'est un point de départ pour la mise en œuvre d'une architecture *Zero Trust* en environnement Microsoft.

Le contrôle d'accès conditionnel et l'authentification forte sont généralisés pour tous les utilisateurs. La solution Microsoft Cloud App Security, couplée à Identity Protection, est utilisée pour la supervision des sessions.



Chemin typique de l'accès des utilisateurs

On restreint ici explicitement l'utilisation des comptes à privilèges (qui sont marqués comme sensibles) à des appareils spécifiques avec le contrôle d'accès conditionnels avec Azure AD Premium.

Sur les postes de travail, un EDR (*Endpoint Detection and Response*) est déployé, il s'agit de Microsoft Defender for Endpoint qui est capable d'interagir avec Azure AD, à travers le MDM, pour remonter l'état de santé des appareils.

La gestion des postes de travail et le déploiement des profils de sécurité est faite avec le MDM Microsoft Endpoint Manager.

Sur les profils de postes « spécialisé » et « administration », l'utilisateur de l'appareil n'est plus administrateur de son poste.
De plus, la liste des applications autorisées à s'exécuter est restreinte.

Enfin, les principes de moindre privilège et le *just-in-time access* (élévation temporaire) des droits d'administration avec Azure AD Premium est mis en œuvre.

Cette implémentation de référence permet ici d'administrer les ressources dans le *cloud* mais également les actifs critiques comme l'Active Directory au travers d'intermédiaires (VPN, serveur de rebond, etc.).

Sécuriser le Tier 0 et mettre en œuvre le plan de contrôle

Quelle que soit la raison qui amène à lancer un projet de renforcement de la sécurité de l'AD (plan d'action consécutif à un incident de sécurité majeur, résultats de tests d'intrusion ou d'exercice de *red team*, etc.), une importante phase préparatoire est nécessaire avant le lancement d'un aussi vaste programme. Il apparaît prioritaire de se focaliser sur le Tier 0 et tenir compte au vu des transformations du SI sur les autres Tiers (utilisation du *cloud* et Azure AD).

Étape 1 : se préparer - 1 à 6 mois

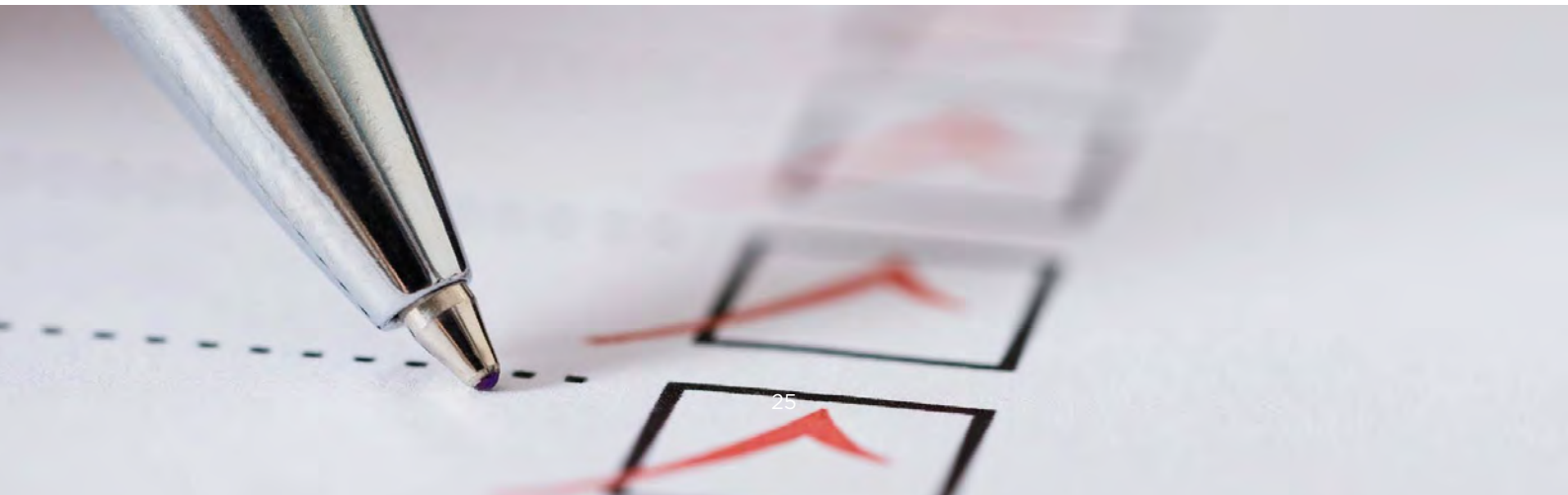
Même si les grandes lignes sont globalement connues en démarrant un projet de sécurisation de l'AD, il est indispensable de délimiter les contours du projet.

La durée de la phase de cadrage dépend bien sûr, en premier facteur, de la complexité de l'environnement. Du cas simple d'une unique forêt AD avec un seul domaine, exploitée par une équipe centrale, au cas déjà plus complexe d'une grande organisation, présente sur toutes les plaques géographiques, ayant vécu de nombreuses acquisitions qui ont conduit à la création de relations d'approbation entre de très nombreuses forêts, les enjeux de chaque projet sont uniques.

> *La sécurisation du Tier 0 est nécessaire, le travail mené ne sera en rien perdu, même en cas de transformation cloud*

Les trois principaux objectifs de la phase de cadrage sont :

1. Dresser une cartographie de l'environnement existant (forêts et relations d'approbation associées) et identifier les vulnérabilités présentes.
2. Déterminer la cible de sécurité à atteindre et l'échéance (*e.g.* périmètres prioritaires, niveau de durcissement à la cible, caractère dédié des infrastructures, forêts dont le décommissionnement est possible, élimination des adhérences entre le système de sauvegarde de l'AD et l'AD lui-même, etc.).
3. Définir la structure projet permettant d'atteindre les objectifs fixés dans le planning défini.



C'est également dans ces phases que l'on prend en compte les plans d'action préexistants (rapports de l'Inspection Générale, audits réalisés, bilan de *red team, etc.*) pour les réintégrer dans ce projet désormais global.

Pour établir la cartographie, l'approche repose sur :

/ des outils reconnus du marché (e.g. PingCastle, BloodHound, OAADS, etc.) ou des *frameworks* (*e.g.* points de contrôle de l'ANSSI) ;

/ des entretiens avec les relais dans les métiers ou les géographies, permettant d'identifier des infrastructures Active Directory autonomes et potentiellement non repérées par les outils.

Une fois tous les éléments rassemblés, les objectifs du projet de transformation sont définis et les trajectoires pour y parvenir établies. Ce type de projets se décompose habituellement en plusieurs sous-chantiers.

Rationaliser les infrastructures (forêts et domaines à décommissionner ou à migrer) et les relations d'approbation lorsque cela est possible.

Durcir et corriger les vulnérabilités identifiées : mise à jour des actifs dont l'OS n'est plus supporté, durcissement système et AD, application régulière des correctifs de sécurité, etc.

Mettre en œuvre le modèle en *Tiers* (prioritairement le Tier 0), et déploiement des modifications d'architecture à apporter (cloisonnement, déploiement d'actifs dédiés au Tier 0, implémentation de postes d'administration dédiés, recours à des silos d'administration…).

Définir le RACI et le modèle d'administration : activités des équipes, type de comptes à privilèges qui leur seront fournis et cinématiques d'administration.

Préparer la reconstruction, avec l'externalisation des sauvegardes sur des systèmes sans adhérence avec Active Directory, tests de reconstruction, etc.

Préconisations pour l'utilisation d'outils publics

De nombreux scripts ou outils *open-source* sont disponibles sur Internet pour évaluer le niveau de sécurité d'un environnement Active Directory / Azure AD. Il convient cependant de respecter quelques règles de prudence avant de les exécuter :

1. Revoir le code source de l'outil, pour s'assurer de son comportement (quand cela est possible).
2. Exécuter l'outil avec le minimum de privilèges requis, selon le principe du moindre privilège, et dans un environnement restreint (machine virtuelle dédiée par exemple).
3. Limiter les flux sortants selon les besoins (pas de flux vers Internet pour une revue de configuration Active Directory, uniquement vers les ressources Microsoft pour une revue Azure AD)

Faut-il mettre en place une forêt d'administration ?

Comme expliqué précédemment, ce modèle n'est plus recommandé par Microsoft, sauf cas particuliers décrit ici, car complexe et coûteux à mettre en œuvre.

Quid de l'administration de l'infrastructure de virtualisation hébergeant les actifs du Tier 0?

La criticité de l'infrastructure hébergeant les actifs du Tier 0 impose qu'elle soit dédiée et que son administration soit intégrée au Tier 0. En effet, l'utilisation d'une plateforme mutualisée fait naître un risque de mauvaise maîtrise des accès à ces machines virtuelles.

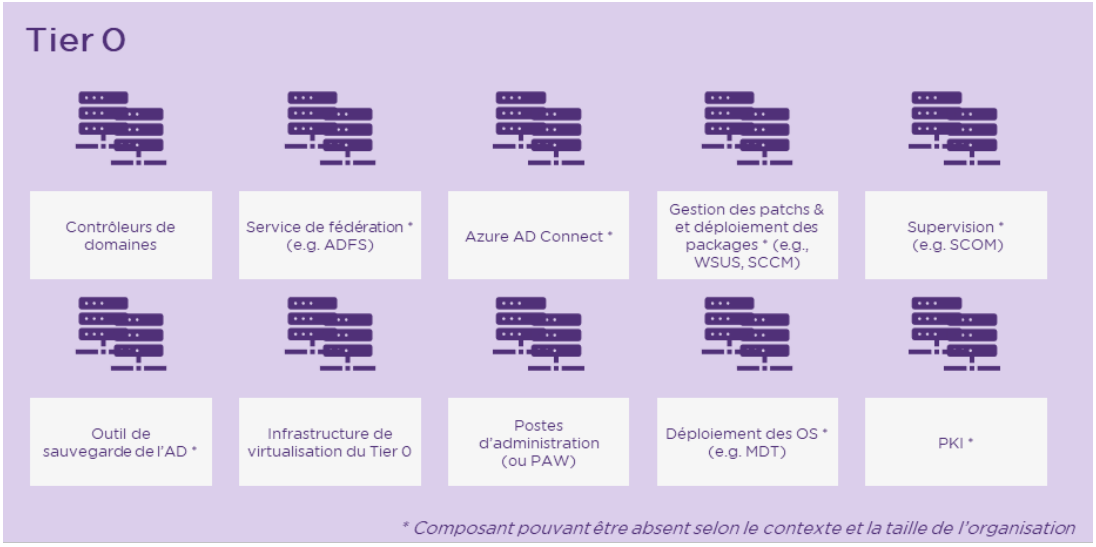
Cependant, la mise à disposition d'une infrastructure dédiée peut être assez longue dans certaines organisations. Pour réduire le risque plus rapidement, l'on pourra utiliser une infrastructure mutualisée existante de manière tactique, afin de débuter sans tarder la mise en œuvre des actions de sécurisation décrites dans la partie suivante.

Une migration sur l'infrastructure dédiée cible, quelques mois plus tard, achèvera de couvrir le risque résiduel mentionné précédemment.

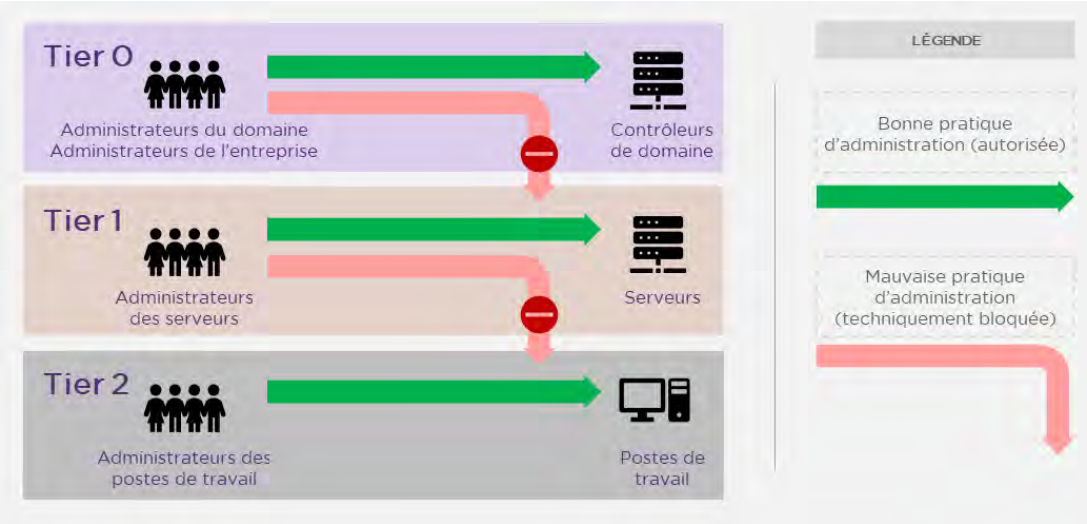
Étape 2 : mettre en œuvre le tier 0 - 6 à 24 mois

Au démarrage de cette étape, les derniers ateliers de réflexion sont menés, pour affiner les cibles à atteindre sur la base du cadrage, embarquer les équipes et présenter le séquencement des actions.

L'identification des différentes équipes d'administration de l'organisation (*e.g.* support IT, équipes AD, équipes serveurs, équipes postes de travail, etc.), de leurs responsabilités et activités, des droits qu'elles doivent avoir pour les réaliser (principes du moindre privilège). Cela permet de définir un RACI clair et de préparer les futurs comptes qui seront utilisés, en lien avec le modèle de délégation du *Tiering*.



Ensuite, viennent les étapes centrales : application de la structure en Tiers dans l'Active Directory, création des comptes d'administration propres à chaque Tier, déplacement des objets dans les bonnes *Organizational Units* (OU). L'étape finale consiste à interdire la connexion à l'aide d'un compte d'un Tier donné, sur un actif d'un Tier inférieur (comme illustré sur le schéma ci-dessous). Cela peut être mis en place, dans un premier temps, grâce à des GPO dites de « deny logon », puis de manière plus pérenne au travers d'Authentication Policy Silos.



Le déploiement d'une GPO « deny logon » permet d'empêcher techniquement les connexions des comptes Tier 0 aux machines sur lesquelles la GPO est appliquée (Tier 1 & 2). Toutefois, les GPO sont des éléments de configuration client, qui pourraient être désactivés localement par un attaquant (dans le but de piéger un administrateur Tier 0 et induire une connexion sur une machine compromise par exemple). Les GPO « deny logon » protègent donc des erreurs d'administration mais présentent des défauts pouvant les rendre vulnérables en cas d'attaque.

Les Authentication Policy Silos permettent de n'autoriser l'authentification de certains comptes (typiquement les comptes d'administration du Tier 0) que depuis certaines machines (typiquement les postes d'administration). Comparé au mécanisme de blocage par GPO, les Authentication Policy Silos ne reposent plus sur une configuration client mais sur un mécanisme imposé par les services Active Directory. Ce mécanisme permet de plus de couvrir le risque de rejeu d'identifiants du Tier 0 (tickets Kerberos) ailleurs que sur un poste d'administration (devant donc lui aussi être compromis). Cependant, la plus grande complexité de mise en œuvre de cette méthode par rapport à celle des GPO peut inviter à procéder par étape : à court terme, implémenter les GPO, à moyen terme, mettre en oeuvre les *Authentication Policy Silos* comme une façon de renforcer encore le niveau de sécurité.

Enfin, cette étape doit également inclure la définition et le déploiement du poste d'administration (PAW, *Privileged Access Workstation*). Ce poste de travail, ne doit avoir comme unique possibilité que de se connecter au actifs du Tier 0 pour y effectuer les actions d'administration. Il peut donc être durci selon les meilleurs standards, et ne comporter aucun logiciel autre que celui qui permet la connexion à distance.
Ainsi, aucun accès à Internet (exception faite de l'accès au portail *cloud* Azure dans un infrastructure hybride par exemple) ni à la messagerie ne doit être possible, afin de limiter l'exposition de ce poste. En cas de besoin, il faudra prévoir la mise en place d'une zone d'échange entre les environnements bureautique et d'administration.

Les sujets épineux : l'adhérence avec le bastion d'administration préexistant dans l'organisation, avec son modèle déjà établi est parfois source de complexité, en dépit des avantages qu'il offre (c.a.d. facilité d'implémentation de l'authentification multi-facteurs, enregistrement des actions).

Durcissement

Cette partie revient à appliquer les mesures de sécurité partout où cela est possible, pour renforcer le niveau de sécurité.
Couvrir le durcissement des actifs du *Tier* 0 : formalisation et application d'un guide de durcissement, limitation au strict minimum du nombre d'agents sur les actifs du Tier 0, puisqu'ils peuvent constituer un vecteur de compromission. Idéalement, seuls des logiciels natifs de Microsoft (antivirus, sauvegarde intégrée, transmission des évènements grâce à WEF(1), agent de supervision MDI(2), Application Control, etc.) doivent être présents.

D'un strict point de vue de la réduction des risques, la mise en œuvre du modèle en Tiers est prioritaire sur le durcissement, même si elle est plus complexe en raison de son impact sur les pratiques d'administration.

Il faut également veiller à modifier les configurations de ces actifs, pour utiliser les systèmes de MCO/MCS dédiés au Tier 0 (supervision, mises à jour des OS, déploiement de logiciels, etc.).
C'est également dans cette étape que les actions de remédiation concernant les comptes à privilèges doivent être menées : remplacement des comptes membres des groupes *Built-In* par des comptes avec droits respectant le principe du moindre privilège, cartographie des comptes de services, recours à MSA/gMSA (*Managed Service Account*) lorsque cela est possible, identification et mise en quarantaine des comptes inactifs, activation de LAPS, etc. Pour se guider, on pourra s'appuyer sur la liste des points de contrôle Active Directory mis à disposition

(1) *Windows Event Forwarding* (2) *Microsoft Defender for Identity*

par l'ANSSI, afin de rehausser le niveau de sécurité par paliers.

Les sujets épineux : les comptes de services de certaines solutions qui exigent, souvent par simplicité, d'être membre des groupes *Domain Administrators* ou *Enterprise Administrators*. Les comptes dont on ne connaît pas l'appartenance et dont on a du mal à estimer l'impact en cas de coupure. La mise en œuvre d'un processus fiable de traitement des comptes inactifs, au-delà du traitement manuel et en masse au moment du projet.

Sauvegarde

La sauvegarde et la restauration des machines est un sujet globalement maîtrisé dans les organisations. Pourtant, il est nécessaire de réétudier cette question à la lumière de la menace actuelle et du scénario du pire : la compromission et destruction totale de l'Active Directory et de ses sauvegardes. Bien souvent, l'infrastructure de sauvegarde est elle-même liée au domaine AD qu'elle sauvegarde.

Malgré ce programme de sécurisation, il est important de rester modeste et de toujours envisager qu'une compromission est possible (« *Assume breach* »). Ainsi, il s'agit de compléter le dispositif de sauvegarde en place, que l'on conservera pour sa performance de son temps de restauration, par un dispositif de sauvegarde externalisé et décorrélé de l'AD.

Détection

Une fois le modèle en Tiers en place, les modes d'administration étant connus et normés, l'on peut mettre en place des scénarios de détection pour identifier les pratiques qui s'écartent du modèle (*e.g.* ajout de compte dans les groupes *built-in*, modification de configurations sensibles et normalement stables de l'AD, utilisation de comptes d'urgences, etc.). Enfin, la mise en œuvre de scénarios de détection de techniques d'attaque (e.g. récupération de *hashs*, nombre important de demandes de tickets Kerberos dans un laps de temps court, etc.). Microsoft fournit une liste de base d'évènements AD à collecter. Évidemment, des processus de traitement des alertes et des incidents doivent être décrits et opérationnels.

Les sujets épineux : la méthode de collecte (utilisation de WEF) qui peut être différente du standard défini par le SOC (collecte par agent installé sur l'actif) et nécessiter des adaptations.

Rationalisation

En parallèle de ces actions de sécurisation, il convient de suivre le bon déroulement du plan de décommissionnement ou de migration défini dans la phase de cadrage.

Un décalage de planning se traduirait immédiatement en un risque important, dans la mesure où aucune action de sécurisation ne serait menée sur ces périmètres. Et d'autant plus s'ils possèdent des relations d'approbation avec les autres forêts.

Les sujets épineux : l'incertitude des impacts précis lors la coupure des relations d'approbation et du décommissionnement.

Pilotage du programme, conduite du changement et reporting.

Pour être exhaustif, il apparaît indispensable de mentionner toutes les activités transverses inhérentes au pilotage du programme. La planification, la synchronisation des équipes et la communication aux parties prenantes sont des éléments clés, compte tenu du nombre important d'actions techniques à mettre en œuvre, de leur interdépendance et de leur impact potentiel.

Par ailleurs, le changement important dans les pratiques d'administration (e.g. utilisation de comptes d'administration distincts par Tier, utilisation d'un PAW) imposé par la mise en place du modèle en Tiers, induit d'apporter une attention toute particulière à la conduite du changement, pour éviter de perturber les activités.

Enfin, il est essentiel de s'assurer que la communication et le *reporting* sur l'avancement du programme soient suffisamment simplifiés et expliqués pour éviter de susciter des frustrations et des incompréhensions au sujet des inévitables points de blocages et demandes d'arbitrages.

Les sujets épineux : la difficulté de faire le lien entre la réalisation d'actions techniques et la couverture des risques, l'importante mobilisation qui est demandée aux équipes en charge du run de l'AD pour mettre en œuvre les actions techniques.

Etape 3 : garantir la pérennité – 1 à 3 mois

Plus que n'importe quel autre composant du SI, la sécurité de l'AD ne peut se réduire à un programme limité dans le temps, mais doit se transformer en un processus régulier de contrôle du niveau de sécurité global. Celui-ci doit être exécuté régulièrement, et les écarts identifiés doivent se traduire par des actions correctrices à court terme et de prévention à moyen terme.

Ce plan de contrôle peut s'appuyer sur diverses sources : des scripts, des outils du marché complémentaires , le service ADS (Active Directory Security) de l'ANSSI, des vérifications manuelles (lorsqu'elles ne peuvent pas facilement être automatisées). Aussi, l'on pourra aussi s'appuyer sur des audits et des exercices de *red team* annuels, pour vérifier que le Tier 0 ne peut plus être compromis.

Enfin, en plus de vérifier que les sauvegardes de l'infrastructure Active Directory réussissent systématiquement, il convient, comme dans toute approche de continuité, de tester la restauration complète depuis une sauvegarde.

Ces tests réguliers permettront aussi de mesurer le délai nécessaire à la restauration complète. Celui-ci pourra être communiqué aux responsables de la continuité et constituera également un indicateur que l'on cherchera à optimiser, test après test.

SYNTHÈSE : Sécuriser le Tier 0

Rationaliser et décommissionner
Focaliser le travail sur les périmètres pérennes et décommissionner le reste.

Mettre en œuvre le *Tier 0*
Cloisonner l'Active Directory, pour le risque de compromission.

Maintenir les composants en condition de sécurité
Appliquer les correctifs de sécurité et durcir les configurations.

Sauvegarder et s'entrainer à restaurer
Mettre les sauvegardes hors de portée et se tenir prêt à reconstruire.

Piloter les actions et conduire le changement
Suivre et déployer rigoureusement ce plan d'action.

Centraliser les logs et mettre en œuvre la détection
Surveiller et détecter les signaux faibles, pour réagir rapidement.

Sécuriser sa souscription Azure AD

L'Identity Secure Score, une première étape

Le degré de sécurisation (ou *Identity Secure Score*) est un indicateur natif permettant de comparer la posture de l'organisation vis-à-vis des bonnes pratiques de Microsoft concernant la sécurisation des identités.

Ce score a été Introduit en 2020, sur base du Microsoft Secure Score présenté fin 2017.

Les principes du calcul sont les suivants :

/ Pourcentage de mise en place des contrôles proposés par Microsoft
/ Les contrôles mesurés dépendent de l'architecture de l'identité et des licences disponibles (cf. tableau ci-dessous)
/ Une seule licence de sécurité active l'apparition du contrôle

Si tous les contrôles sont disponibles pour l'organisation, la répartition du score est la suivante à l'heure actuelle :

/ 61 points sur les identités *cloud* (Paramétrage Azure AD, Accès Conditionnel, Réinitialisation du mot de passe en libre service, Azure AD Identity Protection)
/ 58 points sur les identités locales (avec Microsoft Defender for Identity)

Deux cas peuvent expliquer une évolution : la modification de la posture de l'organisation ou la modification des contrôles par Microsoft.

Il est possible d'en suivre les raisons en regardant les changements affectant le Microsoft Secure Score dans le Centre de Sécurité Microsoft 365.

A noter, le Microsoft Secure Score ne reprend pas tous les contrôles de l'Identity Secure Score.

Dans le cas d'une organisation hybride, sans licence Microsoft Defender for Identity, les contrôles sont les suivants :

Licence	Contrôles	Pondération	Microsoft Secure Score
Gratuite	Désigner plus qu'un Administrateur Général	1	x
Gratuite	Ne pas autoriser les utilisateurs à déléguer leur consentement	4	x
Gratuite	Utiliser des rôles administrateurs limités	1	x
Gratuite	Activer Password Hash Sync	5	x
Gratuite	Ne pas faire expirer les mots de passe	8	x
Gratuite (P1)	Bloquer l'authentification basique	8	x
Gratuite (P2)	Enrôler tous les utilisateurs pour l'authentification forte	9	x
Gratuite (P2)	Exiger le MFA pour les administrateurs	10	x
Azure AD P1	Activer le *self-service password reset*	1	x
Azure AD P2	Activer les politiques *user risk*	7	x
Azure AD P2	Activer les politiques *sign-in risk*	7	x

Gratuite (P1 ou P2) : Besoin d'avoir une licence premium pour personnaliser les mesures de sécurité

Aller plus loin que le Secure Score

L'Identity Secure Score donne une métrique de la posture de l'organisation par rapport à des bonnes pratiques de Microsoft, non exhaustives mais indispensables.

Il est en outre primordial de s'assurer que l'ensemble des paramétrages d'Azure AD soient cohérents avec les enjeux de l'organisation (e.g. domaines autorisés pour les invités). Quelques heures sont suffisantes pour les passer en revue et définir des axes d'amélioration concrets.

Au-delà des configurations de la plateforme, il est plus que recommandé de mettre en place un plan de contrôle permanent afin de suivre les objets qui ne vont pas manquer de se multiplier (applications *cloud* ou *on-premises*, utilisateurs internes et externes, politiques d'accès conditionnel, etc.).

Ce plan de contrôle permettra d'assurer le maintien en condition opérationnelle et de sécurité d'Azure AD au même titre que les plans existants pour les AD locaux.
Au programme, ces contrôles devront reprendre les sujets suivants :

Administrateurs :
- Listes et droits utilisés
- Utilisation des comptes bris de glace

Applications Azure AD :
- Personnes habilitées à enregistrer une application
- Gestion des propriétaires, secrets et des permissions pour chaque application

Accès conditionnel :
- Evolution dans les politiques d'accès
- Gestion des exceptions

Utilisateurs internes :
- État de l'enrôlement des facteurs d'authentification
- Listes et droits utilisés
- Rattachement à une entité

Appareils :
- Conformité des appareils
- Nombre d'appareils par utilisateur

Utilisateurs invités :
- Légitimité du compte
- Droits et permissions associés

Comprendre les rôles dans Azure AD

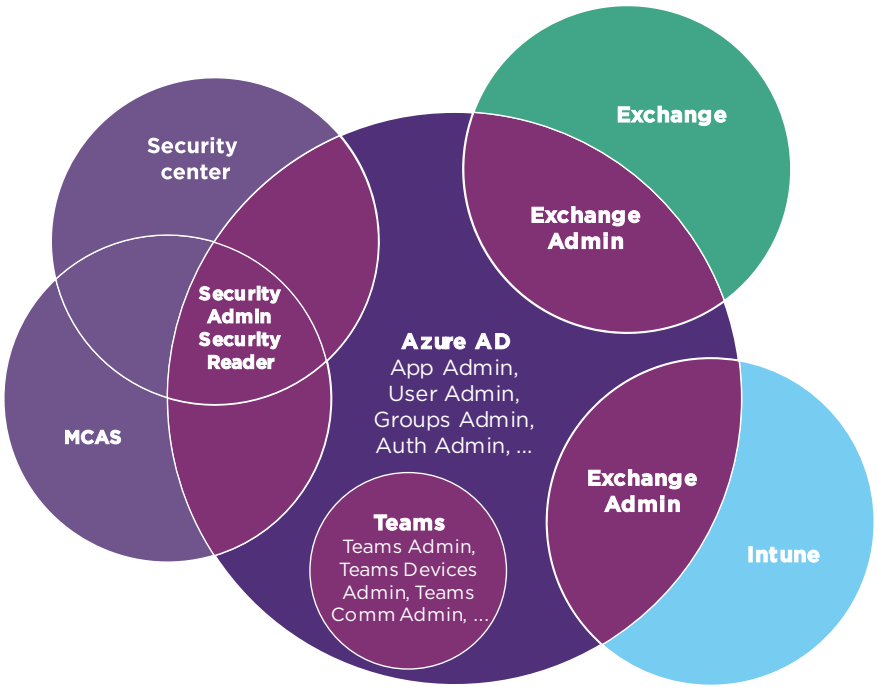
Les rôles Azure AD constituent un élément important dans le dispositif de sécurité du *cloud* Microsoft. Il existe plus de 70 rôles intégrés qui s'appliquent aussi bien à la gestion des ressources de l'annuaire Azure AD mais également à certains services Microsoft 365 (SharePoint Online, Exchange Online, Teams, AIP…) et Azure (Azure DevOps…). Pour aller plus loin, il est envisageable de créer ses propres rôles avec les rôles personnalisés.

Le diagramme suivant illustre les rôles propres à Azure AD, ainsi que des rôles s'appliquant à d'autres services Microsoft 365.

Par défaut, les ressources Azure AD et Azure sont sécurisées de façon indépendante les unes des autres. Néanmoins, un administrateur général Azure AD peut élever son accès pour gérer tous les abonnements et ressources dans Azure.

Cet accès plus élevé, à travers le rôle administrateur de l'accès utilisateur (ou *User Access Administrator*) lui permet d'interagir avec tous les abonnements Azure faisant confiance à son tenant Azure AD. Ainsi, avec ce rôle un administrateur général peut donner à d'autres utilisateurs un accès aux ressources Azure.

Compréhension des rôles ayant des droits au-delà d'Azure AD



Comprendre les applications dans Azure AD

Parmi les identités gérées dans Azure AD, les applications représentent un point essentiel à appréhender et sont très différentes de ce qui existait *on-premises.*

Inscription d'une application

Une application qui souhaite externaliser l'authentification vers Azure AD doit être déclarée dans Azure AD (via *application registration*), qui enregistre et identifie de manière unique l'application (AppId) dans l'annuaire à travers la notion d'objet d'application (ou *application object*).

Cette inscription (ou *application registration*) se fait dans le tenant du propriétaire de l'application. (e.g. Exchange Online est inscrit dans le *tenant* de Microsoft) .
Le propriétaire de l'application peut ensuite déclarer des API qui seront utilisées par l'application (e.g. lire et écrire un mail dans Exchange Online).

En fonction de sa configuration, l'application pourra ensuite être utilisée soit dans son *tenant* soit dans un *tenant* externe.
Pour cela, l'objet application est utilisé en tant que modèle pour créer un ou plusieurs objets principal de service. Un principal de service est créé dans chaque locataire dans lequel l'application est utilisée.

Il est important de noter qu'un administrateur du *tenant* dans lequel est inscrite l'application peut ajouter des authentifiants (secrets ou certificats).

Une personne en possession des authentifiants pourra utiliser les permissions de l'application.

Une application est représentée dans Azure AD par 2 classes d'objets :

- *Objet d'application* : stocke les informations relatives à l'application
- *Objet Service Principal* : représente une instance de l'application.

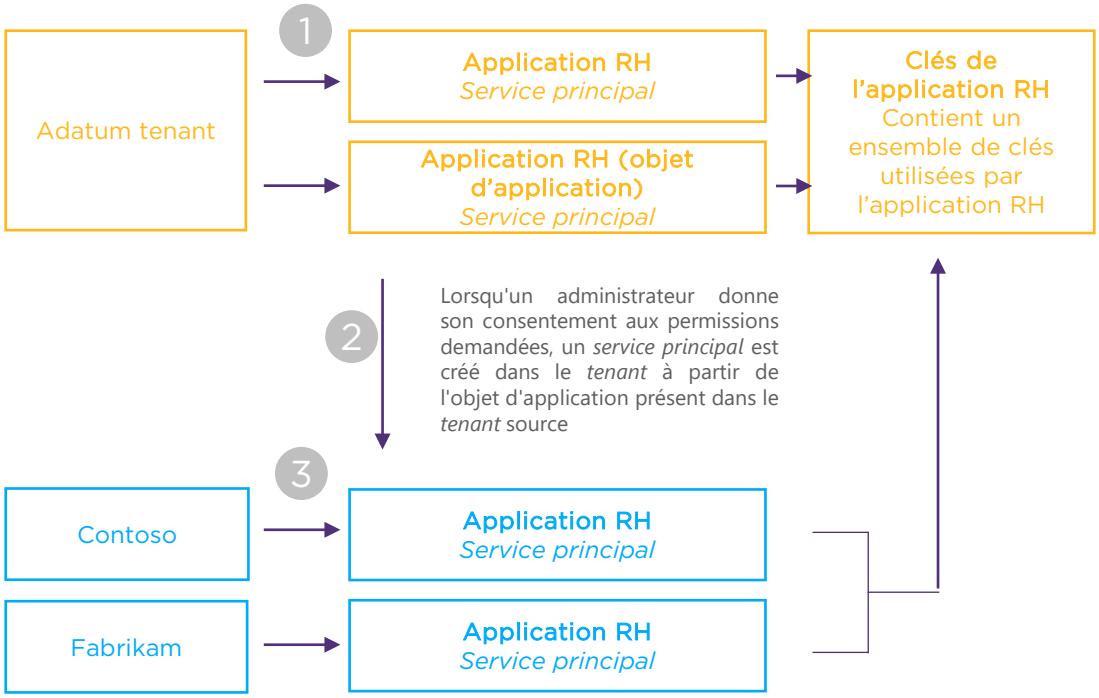
Service Principal

Afin de consommer des ressources protégées par Azure AD, il est nécessaire de s'authentifier soit via un utilisateur ou une application, également appelé principal de service (ou *service principal*).

Les principaux de service sont un type d'objet qui existe dans Azure AD pour représenter une application.

En particulier, un principal de service est généralement créé lorsque vous avez une application ou un code qui doit accéder à des ressources ou les modifier, ce qui ne peut être facilité que par une identité disposant des autorisations nécessaires. La création d'une identité pour une application permet aux administrateurs de lui attribuer des rôles et des autorisations.

Application et principal de service



Il existe trois types de principal de service :

/ **Application** : Instanciation d'une application faite par un administrateur ou par un utilisateur en cas de consentement aux permissions demandées.

Lorsque l'app est déclarée en multi-tenant , alors un principal de service est créé dans chaque tenant ajoutant l'application (avec un identifiant ObjectId propre différent).

Ceci permet d'appliquer des politiques et permissions spécifiques mais aussi l'authentification et autorisation propre a chaque tenant.
Ce SP dans chaque autre *tenant* est crée après le consentement.

Un propriétaire d'une instance de l'application a la possibilité d'ajouter des authentifiants.

/ **Identité gérée** (ou *Managed Identity)* : Identité utilisée par un service Azure pour obtenir un jeton Azure AD sans avoir à manipuler de secret d'authentification.

Il est nécessaire de revoir régulièrement les applications d'entreprises inscrites, les permissions consenties et les authentifiants associés

/ **Hérité** : Principal de service historique similaire aux applications, mais ne pouvant être présent que dans un tenant (non recommandé).

Sécuriser les comptes de services

Un défi courant lors de la création d'applications Cloud est de savoir comment gérer les authentifiants dans le code.
Idéalement, ils ne sont jamais manipulés sur les postes des développeurs et ne sont pas présents dans le code source des applications.

Il existe trois types de compte de service dans Azure AD :

- ***Managed Identity*** : recommandé si le service est natif à Azure
- ***Application*** : recommandé si le service n'est pas natif à Azure ou est multi-tenant
- **Compte utilisateur dédié** : non recommandé (si l'application supporte OAuth)

Recommandations communes
Quel que soit le type choisi, il convient de définir un cycle de vie (création, revue et suppression) et suivre le principe du moindre privilège :

- Préférer les permissions OAuth2 (e.g. lire les fichiers) plutôt que les rôles natifs Azure AD (e.g. administrateur SharePoint Online)
- Utiliser des comptes de services différents pour des permissions différentes
- Dans le cas d'Exchange Online et SharePoint Online, il est également recommandé de limiter par élément les applications autorisées.

Protéger les authentifiants des applications

Étant donné que les *service principals* ne supportent pas l'accès conditionnel à l'heure actuelle, le risque est que les authentifiants tombent dans de mauvaises mains.

Pour s'en prémunir, il faut :

- Utiliser uniquement des applications créées dans son *tenant*
- Stocker les secrets dans Azure Key Vault

Deux types de *Managed Identity*
Une identité gérée attribuée par le système est activée directement sur une ressource Azure. Lorsque la ressource est activée, Azure crée une identité pour la ressource dans le tenant Azure AD. Une fois l'identité créée, les informations d'identification sont provisionnées sur la ressource. Le cycle de vie d'une identité attribuée par le système est directement lié à la ressource Azure.

Une identité gérée et attribuée par l'utilisateur est créée comme une ressource Azure autonome. Azure crée une identité dans le tenant Azure AD qui est approuvé par l'abonnement auquel la ressource est associée. Après la création de l'identité, elle peut être affectée à une ou plusieurs ressources Azure. Le cycle de vie d'une identité attribuée par l'utilisateur est géré séparément du cycle de vie des ressources Azure associées.

FOCUS

Comprendre les licences Azure AD et leurs apports sécurité

Il n'est pas possible de parler de la sécurité des identités dans un environnement Microsoft sans évoquer les différents niveaux de licences.

Les éditions Azure AD Premium ajoutent des fonctions d'administration avancées, le contrôle d'accès conditionnel, les groupes dynamiques, la protection des identités, des fonctions en libre-service pour les utilisateurs et également un niveau de service plus élevé (99,99% garanti depuis 2021).

Une autre fonctionnalité d'Azure AD Premium est Application Proxy. Ce service permet aux organisations de raccorder des applications intranet traditionnelles à Azure AD. Ce raccordement se fait via la jonction entre des protocoles modernes (basés sur des revendications d'identités) et des anciens protocoles comme Kerberos ou NTLM.

Pour bénéficier des principales fonctionnalités de sécurité, un utilisateur interne doit avoir une licence comme indiqué ci-dessous :

AZURE AD GRATUITE / O365	AZURE AD PREMIUM P1	AZURE AD PREMIUM P2
Security defaults		
	Intégration avec MIP Réinitialisation de mot de passe en libre service Protection des mots de passe Azure MFA Accès conditionnel (1)	
		Protection des identités (2) Gouvernance des identités (3)

(1) Il est possible de mettre en place un accès conditionnel via un fournisseur d'identité tierce, mais celui-ci ne permettra d'avoir une granularité pour les différentes applications Azure AD ou de gérer les durées de vie des sessions
(2) Protection des identités : Stratégie de risque utilisateur ou en matière de risque à la connexion et Politiques d'accès conditionnel basé sur le risque
(3) Gouvernance des identités : Azure AD PIM, Révisions d'accès, Gestion de packages d'accès

FOCUS

Security Defaults : un niveau de sécurité minimal accessible à tous

Microsoft a introduit en 2019, les *Security Defaults*, des politiques de sécurité prédéfinies par Microsoft permettant d'assurer une posture de sécurité minimale, sans condition de licence :

1. Pour les administrateurs activation d'une authentification multi-facteur à chaque connexion
2. Pour les utilisateurs activation d'une authentification multi-facteur en cas de connexion risquée
3. Pour tous les utilisateurs enregistrement d'un facteur MFA dans les 14 jours suivant leur première connexion
4. Désactivation des protocoles hérités
5. Accès au portail Azure AD seulement pour les administrateurs

Pour personnaliser ces politiques, des licences Azure AD Premium Plan 1 ou 2 sont nécessaires.

Il est à noter que les *Security Defaults* ne peuvent pas être activés en même temps que des politiques d'accès conditionnel.

FOCUS

Quelle gouvernance pour Azure Active Directory ?

Dans un certain nombre d'organisations, la responsabilité de l'Azure Active Directory tombe dans un *no man's land*. Cela est en grande partie dû à l'absence de cible :

/ Simple annuaire technique pour Office 365/Teams ou futur référentiel d'identité pour les applications de l'organisation ?
/ Référentiel d'identité pour les applications *cloud* uniquement ou également pour les applications hébergées en interne ?

Quels acteurs aujourd'hui ?

Dès que l'on parle administration d'Azure AD, trois acteurs sont généralement présents :

L'équipe Identité pour la mise en place de la synchronisation et la fédération ou pour le raccordement d'une application.
Habitués à avoir des droits à importants sur l'Active Directory, ils héritent d'un rôle *Global Administrator*, bien qu'ils ne possèdent pas encore les compétences requises pour ce rôle.

L'équipe *Digital Workplace* pour la configuration des services collaboratifs. Cette équipe a souvent étendu son périmètre au-delà d'Exchange ou de SharePoint Online par opportunité. Bien que la gestion de l'identité ne soit pas historiquement de leur ressort, il s'agit souvent de la seule équipe avec les compétences pour gérer des sujets liés à la collaboration (e.g. invités, accès conditionnel ou applications tierces)

L'équipe Sécurité pour la définition des politiques de sécurité et le contrôle des configurations en place.

Quels principes pour la gouvernance sur Azure AD ?

La logique est similaire pour Active Directory comme pour Azure Active Directory. Le modèle opérationnel doit suivre deux principes fondamentaux : ségrégation des droits et moindre privilège. En somme, **tout ce qui est délégable doit être délégué**.

En revanche, Azure AD ne permet pas le même niveau de délégation que sur Active Directory (où tout peut être délégué en modifiant le schéma), bien que Microsoft ait introduit plusieurs évolutions en ce sens récemment.

Quelles possibilités de délégation ?

Il convient tout d'abord de différencier le **contenant** (Azure AD et les briques d'infrastructure de synchronisation et fédération sous-jacentes) et le **contenu** (identités utilisateurs, applicatives et liées à des terminaux).
Microsoft propose un modèle **RBAC** (Rôle Based Access Control) avec des rôles natifs. Parmi ces rôles, on retrouve des rôles d'administration du tenant Azure AD, des services Office 365 ou des différentes identités. A noter, seul le rôle administrateur général peut être utilisé pour modifier certains paramètres généraux, comme la charte graphique de la page de connexion.

Microsoft a introduit en 2019 la possibilité de faire **des rôles personnalisés** en s'appuyant sur les API. Pour l'instant, seules les actions liées à l'administration des applications sont utilisables lors de la définition d'un de ces rôles.
Il sera également indispensable de garder en tête qu'Azure AD est aujourd'hui pensé comme une **organisation centralisée**, même si Microsoft a publié en 2021 les unités d'administration, équivalent des Unités Organisationnelles (UO) locales, afin de limiter le champ d'action d'un administrateur.

Quels scénarios possibles pour la gestion d'Azure AD ?

Afin de respecter les principes ci-dessus, il est nécessaire d'identifier des équipes avec chacune des responsabilités et des droits qui lui sont propres.
Pour la gestion des contenus, cela n'est pas très compliqué si l'on met de côté le caractère centralisé de la plateforme. Les équipes *Digital Workplace* seront par exemple logiquement en charge des services et données Office 365. **La gestion du contenant reste LA question centrale**.

Une équipe centrale devra être définie avec les droits d'administrateur général. Elle aura pour mission de réaliser toutes les tâches d'administration à très hauts privilèges, qui pourront sortir du périmètre strict de l'identité.

/ Cette équipe devra être **dimensionnée** et **formée**
/ Des **processus avec des SLAs** devront être mis en place

L'équipe centrale n'étant pas en mesure de définir toutes les fonctionnalités accessibles par tel niveau d'administration, la responsabilisation des bonnes équipes sera clé (e.g. la communication pour la charte graphique).
Etant donné que ces droits ne seront utilisés que rarement, il est essentiel de maîtriser qui peut y accéder et quand (via un bastion ou Azure AD PIM).
Un scénario pourrait être de confier cette responsabilité à l'équipe identité afin de maintenir une cohérence avec la gestion des identités et la qualité des données. Un autre pourrait être de former une équipe centrale garante des applications à portée Groupe.

Migrer d'Active Directory vers Azure Active Directory

Dans une stratégie de modernisation, la recommandation de Microsoft est, à terme, de réduire Active Directory au fur et à mesure que les applications et les ressources internes seront disponibles depuis le *cloud*, que ce soit sous la forme d'applications SaaS ou bien tout simplement d'applications existantes.

Alors que les identités vont migrer dans Azure AD, les postes de travail vont quitter Active Directory pour être gérés depuis un service MDM dans le *cloud*. Cette bascule va avoir pour effet de progressivement limiter son exposition aux attaques.

La gestion des identités avec un service *cloud* comme Azure AD est plus simple à appréhender (moins de concepts à maîtriser et pas de composants d'infrastructure à mettre à jour).

En migrant vers Azure Active Directory, il est plus simple de bénéficier de l'analyse centralisée des événements de connexion, facilitant ainsi la détection des attaques à faibles volumes et également des anomalies de connexion.

Pourquoi joindre un appareil à Azure AD?

Il y a plusieurs intérêts à joindre un appareil à Azure AD :

/ Renforcer le contrôle d'accès conditionnel en se basant sur l'état de santé de l'appareil ou l'emplacement géographique ;

/ Accéder de manière simple et sécurisée aux applications *cloud* avec une expérience SSO à travers l'obtention d'un PRT (Primary Refresh Token) ;

/ Gérer les appareils à l'aide d'une solution de MDM ;

/ Déployer l'authentification sans mot de passe de type Windows Hello for Business ou FIDO2.

Qu'est-ce qu'Azure AD DS ?

Azure AD DS (Azure Active Directory Domain Services) est l'annuaire AD sous la forme d'un service cloud proposé par Microsoft comme il peut exister chez d'autres fournisseurs *cloud*. De manière simplifiée, le Tier 0 est ici géré par Microsoft, tandis que les autres tiers sont gérés par l'organisation. Azure AD DS fournit un sous-ensemble de fonctionnalités Active Directory comme la jonction de domaine, les stratégies de groupe (GPO), le protocole LDAP et l'authentification Kerberos/NTLM.

C'est une solution à envisager pour les serveurs Windows que l'on migre en *lift-and-shift* dans le *cloud* ou bien que l'on souhaite retirer de la forêt AD de production.

FOCUS

Protéger le *cloud* d'une compromission de l'AD

1 Isoler complètement les comptes administrateurs Microsoft 365 et Azure AD

Les comptes administrateurs doivent être :

- Créés depuis Azure AD;
- Authentifiés avec l'authentification multi-facteurs (MFA);
- Contrôlés par l'accès conditionnel d'Azure AD;
- Accessibles uniquement en utilisant des postes de travail gérés dans Azure;
- Activés sur une plage de temps limitée avec Azure AD PIM.

2 Aucun compte Active Directory ne doit disposer de privilèges élevés sur le *cloud*

Assurez-vous que ces comptes, y compris les comptes de service, ne sont pas inclus dans les rôles ou groupes privilégiés du *cloud* et que les modifications apportées à ces comptes ne peuvent pas avoir d'impact sur l'intégrité de votre environnement *cloud*. Les éléments *on-premises* du Tier 0 ne doivent pas être en mesure d'avoir un impact sur les comptes ou rôles privilégiés de Microsoft 365.

3 Gérer les appareils des administrateurs à partir du *cloud*

Utiliser Azure AD Join et la gestion des appareils de type MDM dans le *cloud* pour éliminer les dépendances à l'infrastructure de gestion des appareils *on-premises*, qui peuvent compromettre les mesures de sécurité des appareils servant à administrer le *cloud*.

4 Utiliser l'authentification Azure AD pour éliminer les dépendances vis-à-vis de l'AD

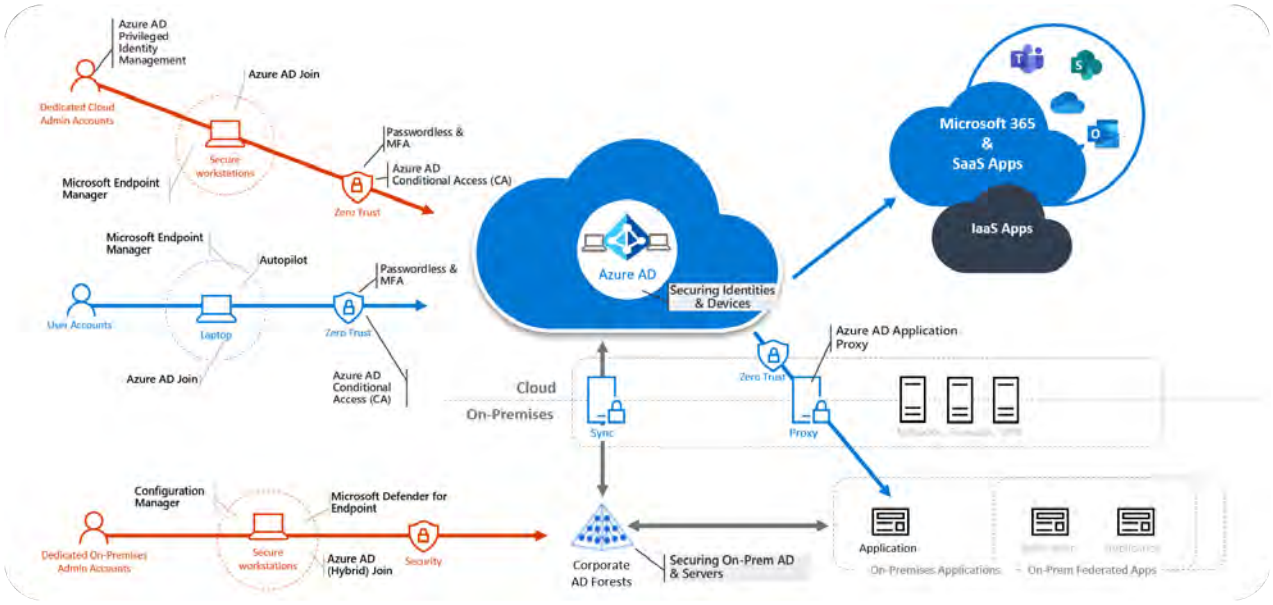
Utiliser toujours une méthode d'authentification forte, telle que Windows Hello for Business, FIDO2 ou Microsoft Authenticator.

Passer à une méthode d'authentification sans mot de passe et envisager de supprimer les mots de passe sur ces comptes.

Le voyage vers Azure AD

Lorsque l'on évoque, un projet de migration vers Azure AD, il est naturel de se poser la question suivante : « Quand Azure AD pourra-t-il remplacer complètement Active Directory » ? Bien qu'il soit tentant de chercher une date précise, il faut garder à l'esprit qu'Azure AD n'est pas « Active Directory dans le *cloud* » et que, de ce fait, il ne faut pas chercher à retrouver les mêmes fonctionnalités.

Cette transition devrait prendre plusieurs années, tant du côté des organisations que pour Microsoft. À l'heure actuelle, toutes les technologies ne sont pas encore disponibles pour passer à un déploiement « *100 % cloud Azure AD* ».



Pour ne pas tomber dans le piège d'attendre qu'une solution parfaite soit disponible (couvrant tous les cas de figure), le mieux est d'aborder ce voyage vers Azure AD dès maintenant, et de façon pragmatique sans chercher à couvrir tous les cas.

Schématiquement, un annuaire Active Directory contient des appareils, des applications et des utilisateurs. La trajectoire de migration va prendre en compte ces trois éléments, afin de les déplacer au fur et à mesure dans Azure AD.

Les organisations ayant un existant fort avec Active Directory auront une trajectoire de migration vers Azure AD qui sera plus ou moins rapide, en fonction du nombre d'objets à migrer mais également de la complexité de l'environnement AD comme le nombre de forêts existantes.

FOCUS

Se moderniser sur trois piliers

Appareils

Placer les postes de travail Windows 10 existants, en mode *Hybrid Azure AD Join*

Joindre nativement à Azure AD, les nouveaux postes Windows 10/Windows 11 à l'aide de Windows Autopilot

Applications

Migrer, dans la mesure du possible, l'authentification des applications dans Azure AD

Migrer les serveurs de fédération AD FS vers Azure AD

Migrer vers Azure AD DS les applications trop anciennes basées sur NTLM et ne pouvant migrer sur des protocoles plus modernes

Utilisateurs

Généraliser l'authentification forte et sans mot de passe pour tous les utilisateurs

Déployer le nouvel outil Azure AD Connect Cloud Sync qui simplifie la gestion en centralisant la configuration dans Azure AD, facilite les déploiements en haute disponibilité et donne accès aux nouveaux scénarios comme le support des environnements multi-forêts AD en mode déconnecté

Quelle trajectoire de modernisation ?

Pour les organisations qui font choix de la modernisation vers le Cloud, la transition vers Azure AD est progressive, par étapes : en synchronisant les utilisateurs, en migrant les postes de travail, en intégrant les applications dans Azure AD puis en migrant les serveurs d'application éligibles dans le *cloud*.

Au fur et à mesure, le contenu de l'Active Directory est réduit et simplifié. La priorité est de migrer respectivement le Tier 2 et le Tier 1 dans Azure AD et Azure AD DS.

Le centre de gravité se déplace vers Azure AD qui devient le plan de contrôle Zero Trust et l'environnement où les ressources sont d'abord créées puis synchronisées si besoin en local vers Active Directory.

L'Active Directory est isolé progressivement pour servir uniquement les scénarios critiques et les applications qui ne peuvent pas migrer vers le *cloud*. Le seul investissement pérenne est la mise en place du Tier 0 et le durcissement de la configuration Active Directory.

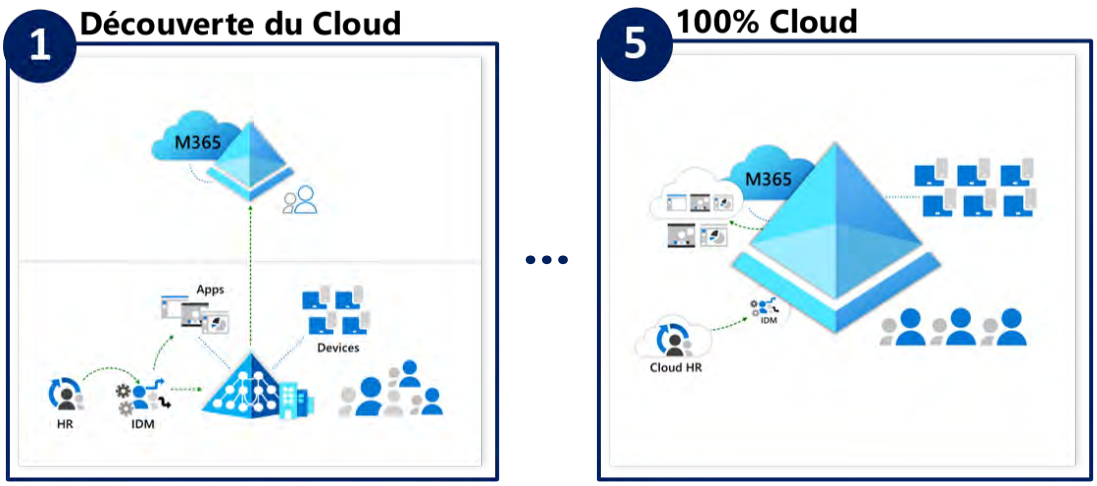
Dans cette transformation, les appareils ne sont plus présents dans Active Directory mais directement intégrés dans Azure Active Directory et gérés par des solutions modernes de type MDM.
En intégrant les applications dans Azure AD, l'approche sécurité se modernise : notamment en publiant les applications IaaS et *on-premises* qui n'ont pas encore migré vers le *cloud*, à travers Azure AD Application Proxy.

Rendre les applications accessibles depuis Internet de manière sûre, sans recourir à un réseau privé virtuel (VPN), est un changement majeur pour de nombreuses organisations même si le *split-tunneling* est une approche de plus en plus courante.

Pour les applications qui ont une dépendance forte à Active Directory, une piste à privilégier est de migrer ces applications vers Azure AD Domain Services.

Azure AD devient l'annuaire de référence depuis lequel les identités sont synchronisées vers les référentiels tiers, comme l'AD en local.

Au fil du temps, l'Active Directory devient une préoccupation moins importante, avec la diminution du nombre d'actifs gérés.



Les étapes en détails

La progression d'un projet de transformation Active Directory vers Azure AD peut se mesurer à l'aide des étapes suivantes :

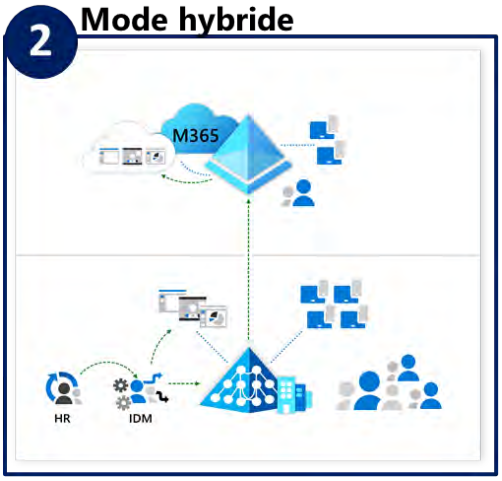
1. Premiers pas vers le *cloud* et utilisation d'Azure AD
2. Généralisation du mode hybride
3. Investissements centrés sur le *cloud*
4. AD isolé et réduit au minimum
5. 100% *cloud* – Azure AD

Premiers pas

Pour accéder à Office 365 et plus globalement aux services du *cloud* Microsoft, les organisations possèdent un tenant Azure AD qui contient *a minima* les objets utilisateurs.

Il s'agit de l'état de toute organisation ayant commencé à utiliser le *cloud* Microsoft : un annuaire Active Directory on-premises ; des appareils joints à AD dont la configuration est faite à l'aide de stratégies de groupes (GPO); des applications *on-premises* utilisant l'authentification intégrée AD pour contrôler l'accès des utilisateurs; et enfin des utilisateurs qui sont créés dans l'AD à partir de systèmes RH puis sont synchronisés d'AD vers Azure AD à l'aide de l'outil Azure AD Connect.

Mode Hybride



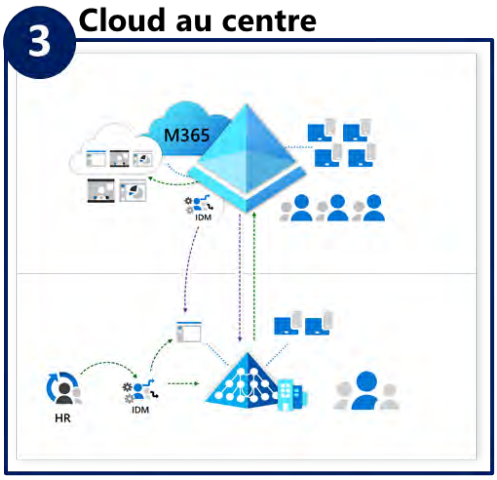
La prochaine étape, que de nombreux clients explorent actuellement, consiste à devenir hybride et à **tirer parti des services de sécurité disponibles dans Azure AD** dans la version de base mais également dans les versions Premium comme l'authentification sans mot de passe, le contrôle d'accès conditionnel, la gestion des identités privilégiées ou bien la réinitialisation du mot de passe en libre-service pour les utilisateurs.

Les appareils Windows existants sont déclarés dans Azure AD à l'aide du mode Hybrid Azure AD Joined, (ce qui facilite le SSO).

Certaines applications sont migrées vers le *cloud* sur une infrastructure IaaS, en s'intégrant à Azure AD Domain Services.

D'autres applications existantes sont toujours hébergées sur site mais sont publiées pour les utilisateurs en télétravail à travers Azure AD App Proxy. Cela permet de donner un accès externe sans VPN tout en protégeant l'accès avec Azure Active Directory.

Être centré sur le *cloud*



Durant cette phase, la décision est prise de ne plus ajouter de nouveaux appareils ou de nouvelles applications dans Active Directory. Les investissements sont en priorité faits dans le *cloud*. Les projets d'intégration avec Active Directory sont ralentis afin d'arrêter d'étendre la dette technique.

La priorité est ici de migrer le Tier 2 et le Tier 1 dans Azure AD.

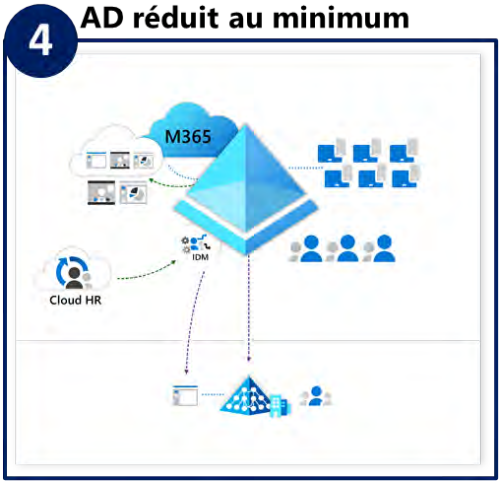
Les organisations cessent dans cette phase d'intégrer les nouveaux appareils dans Active Directory et vont à la place joindre les nouveaux postes de travail directement à Azure AD avec Autopilot et une assurer une gestion par un MDM comme Microsoft Endpoint Manager. Les GPO ne sont plus utilisées pour gérer les nouveaux appareils.

Les applications fédérées sont migrées progressivement vers Azure AD. Elles sont hébergées dans le *cloud* et utilisent Azure AD pour l'authentification. Les applications existantes sont publiées progressivement à travers Application Proxy (et, si nécessaire migrées dans Azure AD Domain Services). Les applications nécessitant d'avoir des profils utilisateurs à synchroniser utilisent le connecteur ECMA.

Les applications existantes utilisent Azure AD DS et sont publiées à travers App proxy.

Les partages de fichiers et les serveurs d'impression sont migrés progressivement vers le *cloud*. Les services Azure Files et Universal Print sont progressivement utilisés.

Isolement de l'AD

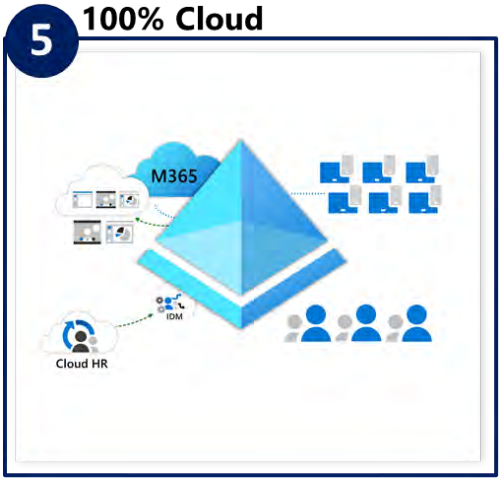


En cible de cette étape, Active Directory doit être réduit à l'administration des ressources internes n'ayant pas vocation à migrer dans le *cloud* (par exemple, systèmes industriels) avec des stations d'administration renforcées, une segmentation réseau et des systèmes de détection garants de la sécurité sur un périmètre désormais excessivement restreint. Si cela n'a pas été réalisé auparavant, la priorité est alors de mettre en place le Tier 0 et de durcir la configuration Active Directory.

Au fur et à mesure, les utilisateurs sont créés et gérés uniquement dans Azure AD avec une stratégie « *Cloud-first* » et sont synchronisés vers Active Directory uniquement si nécessaire à travers la fonctionnalité de *Write-back*.

Le passage à cette étape nécessite de moderniser les applications existantes : en mettant à jour la configuration, le code des applications ou en les remplaçant avec une version *cloud* équivalente. Lorsqu'Azure AD intègrera la capacité d'émission de tickets de service Kerberos, il sera alors possible de continuer à prendre en charge les applications existantes compatibles Kerberos, et ceci sans avoir besoin de comptes utilisateurs dans Active Directory. De plus, les services AD managés comme Azure AD DS aident à supporter les applications existantes sur des serveurs IaaS en proposant le service AD dans le *cloud*.

Full Cloud



Enfin, l'étape 5 est celle du « *100% Cloud Azure AD* », où l'organisation n'a plus aucune empreinte Active Directory. A ce stade, il n'y a plus de contrôleurs de domaine Active Directory et Azure AD fournit tous les outils de gestion des identités.

Les applications authentifient les utilisateurs à travers Azure AD avec des protocoles modernes ou à travers le support de Kerberos avec Azure AD DS et Azure AD. Bien entendu, à ce stade tous les appareils sont joints uniquement à Azure AD et gérés avec un MDM compatible.

Principaux sujets à adresser pour passer en 100% Azure AD

	NTLM	GPO	AD Join
FREIN	NTLM	GPO	AD Join
CIBLE	Kerberos / OpenID Connect	Stratégie MDM	Azure AD join
COMPLEXITÉ	●●●	●○○	●●○

Améliorer sa posture de sécurité

Vous avez dit « Zero Trust » ?

Aborder la cybersécurité sous l'angle de l'identité est une des tendances de fond que les organisations tentent d'adresser à travers l'approche « Zero Trust ». Le principe ? **ne jamais faire confiance, toujours vérifier.**

A chaque demande de connexion, le contexte d'accès est analysé pour évaluer le niveau de confiance que l'on peut accorder à l'utilisateur, à son appareil mais également aux applications.

Cette approche de la sécurité protège les organisations en accordant l'accès sur la base d'une vérification continue des identités et de la posture de sécurité des appareils.

La fin du VPN avec le Zero Trust ?

Une idée fausse et très répandue est que le passage à une architecture « Zero Trust » signifie qu'il est possible de supprimer tous les accès VPN pour l'accès à distance aux ressources de l'entreprise.

La réponse n'est pas aussi simple. Par exemple, si les postes de travail sont *Hybrid Azure AD Join*, alors ces appareils doivent avoir de temps à autre une connectivité vers un contrôleur de domaine, car ils sont joints à Active Directory et Azure AD. L'autorité de référence signant le vérificateur des secrets d'authentification sur l'appareil, pour ouvrir une session en mode déconnecté, est Active Directory. Si le cache des crédentités est vidé ou désynchronisé pour avoir de nouvelles crédentités en cache, l'appareil doit dialoguer avec un contrôleur domaine. Cela doit se faire à l'aide d'une connexion VPN ou sur le réseau de l'organisation.

Autre exemple: lorsque l'utilisateur oublie son mot de passe et demande à le réinitialiser ou le fait lui-même à travers un service de type libre-service, son appareil doit pouvoir joindre un contrôleur de domaine Active Directory pour utiliser le nouveau mot de passe et déverrouiller l'ordinateur.

La même exigence de connectivité *on-premises* est valable lors de la première configuration de Windows Hello for Business sur un appareil *Hybrid Azure AD Join* : l'appareil doit avoir une connectivité vers un contrôleur de domaine pour finaliser la configuration de Windows Hello for Business (définition du code PIN, première ouverture de session avec Windows Hello for Business).

Ces contraintes n'existent pas avec un appareil *Azure AD Join* qui ne nécessite pas de connectivité vers Active Directory contrairement aux scénarios précédents.

La technologie « Always On VPN » , nativement présente à partir de Windows 10, est très utile pour établir un tunnel VPN avant même que l'utilisateur n'ouvre une session et assurer ainsi cette exigence de connectivité interne.
La modernisation du VPN vers une approche plus flexible de type Split-Tunneling augmente les chances de succès à long terme lors de la mise en œuvre d'une architecture Zero Trust.

Encadrer les mots de passe

Le *password spraying* (pulvérisation de mots de passe), une attaque qui donne lieu à un tiers des compromissions de comptes, consiste à tester quelques mots de passe faibles sur un très grand nombre de comptes utilisateurs, plutôt que de nombreux mots de passe courants. La dangerosité de cette attaque est liée au fait que les mesures de sécurité habituelles (blocage des comptes ou temporisation entre des essais successifs) sont inefficaces.

Selon une enquête réalisée par Microsoft auprès de responsables informatiques de plusieurs pays ayant entamé leur voyage Zero Trust, il ressort que 76% ont implémenté en premier lieu une authentification forte et 60% l'accès conditionnel basé sur des politiques.

L'utilisation d'Azure AD, permet de détecter les modèles d'attaque de type password spraying en examinant les tentatives de connexion échouées pour des millions d'organisations dans le monde entier. Cette protection peut être étendue à Active Directory à travers un agent à installer sur les contrôleurs de domaine et en suivant les instructions du guide de déploiement.

Se diriger vers l'authentification sans mot de passe

On observe un engouement important pour l'authentification sans mot de passe. Rien d'étonnant quand on sait que les mots de passe sont responsables de 80% des portes d'entrée pour les pirates et qu'on estime que le déploiement de l'authentification multi-facteur réduit le risque de compromission de 99,9%.

L'authentification s'appuie sur une caractéristique biométrique telle qu'un visage, une empreinte digitale, ou un code confidentiel propre à un appareil et qui n'est pas transmis sur le réseau. Vous aurez le choix entre l'utilisation de votre ordinateur Windows avec biométrie et/ou code PIN, la connexion par clé de sécurité FIDO2 ou l'application Microsoft Authenticator pour les appareils mobiles.

Comment faire face à une cyberattaque ?

Ce chapitre partage les principales difficultés pour reconstruire un Active Directory et propose des actions à mener pour se préparer à une cyberattaque.

Connaitre les difficultés de la reconstruction d'Active Directory pour mieux anticiper la crise

Des effets de bord difficiles à prévoir et à traiter dans de très courts délais

Deux méthodes de reconstruction AD peuvent être mises en œuvre suite à une compromission : une reconstruction à partir de zéro des contrôleurs de domaine et de l'annuaire ou une reconstruction des contrôleurs de domaine mais avec réplication de l'annuaire existant.

La reconstruction consécutive à un incident cyber majeur, est souvent l'opportunité pour la mise en place à marche forcée de mesures de sécurité, par opposition à la méthode « des petits pas » employée dans le cadre d'un projet standard pour ne pas perturber les activités.

La première option permet de s'assurer de la bonne suppression des éventuels moyens de persistance de l'attaquant mais requiert d'importants efforts de reconstruction et une interruption de service importante
À l'inverse, la seconde possibilité permet une reprise du service AD plus rapide, tout en ne garantissant pas de manière certaine l'intégrité de l'annuaire.

Des effets de bords opérationnels, pouvant fortement varier selon l'environnement, sont à prévoir en cas de reconstruction. Lors d'une reconstruction Active Directory à la suite d'une attaque, par exemple de type *ransomware*, des actions de durcissement et remédiation sont prises : ces actions sont souvent mises en œuvre sans phase d'analyse et de tests. Ils peuvent notamment être à l'origine d'effets de bords opérationnels.
Les effets de bords notables suivants peuvent notamment être cités :

- rupture du Secure Channel entre les machines et Active Directory suite à la réinitialisation / restauration de comptes ordinateurs ;
- dysfonctionnement d'applications reposant sur des comptes de service dont le mot de passe a été réinitialisé ;
- invalidation des droits d'accès (ACL) sur les partages de fichiers réseau (en cas de reprise *from scratch* invalidant les SID définis sur les ressources) ;
- nécessité de migrer des serveurs obsolètes ne pouvant plus s'authentifier suite à la désactivation des protocoles d'authentification *legacy*.

Par ailleurs, une absence de vision d'ensemble sur le Système d'Information peut grandement complexifier la

reconstruction (documents numériques détruits, copies physiques obsolètes, connaissances résiduelles partielles, ...). Le temps d'indisponibilité ne dépendra pas uniquement de la complexité des manipulations mais aussi de la capacité à mobiliser suffisamment d'experts et de la priorité donnée à la reconstruction AD (mobilisant des acteurs par ailleurs sollicités pour le maintien d'un éventuel mode dégradé).

« Au moins une semaine est en moyenne nécessaire pour reconstruire le cœur AD sans préparation »

Les ressources internes sont bien souvent mobilisées sur la mise en œuvre d'un mode dégradé, au détriment des efforts de reconstruction. De plus, la possibilité d'un renfort de partenaires n'est pas garantie dans les délais de la crise : peu d'acteurs disposent aujourd'hui du niveau d'expertise pour accompagner opérationnellement les reconstructions AD.

De multiples moyens de persistance discrets

En parallèle de la remise en production du SI, il est nécessaire de s'assurer d'éliminer les moyens de persistance de l'attaquant, pour empêcher une nouvelle compromission de l'environnement.
Les techniques de persistance Active Directory sont nombreuses et difficilement vérifiables dans leur exhaustivité. Si certaines techniques de persistance sont bien connues, et leur remédiation outillée, comme le renouvellement des secrets du compte « krbtgt », d'autres sont plus complexes à détecter et corriger. C'est par exemple le cas des persistances réalisées au travers de permissions et droits étendus spécifiques ou les persistances locales sur les contrôleurs de domaine.

Le CERT-W référence de nombreuses techniques pouvant être utilisées par un attaquant pour maintenir une persistance AD après compromission

Une reconstruction complète de la forêt Active Directory, bien qu'incompatible avec une reprise d'activité rapide, est souvent le seul moyen permettant de s'assurer de l'élimination complète des moyens de persistance AD de l'attaquant suite à la compromission d'un domaine.
Au-delà des contrôleurs de domaine et des annuaires AD en tant que tels, les ressources et serveurs auxquels les contrôleurs de domaine adhérèrent, tels que les serveurs de mises à jour ou l'infrastructure de gestion de clés, ou les serveurs T1, peuvent aussi avoir été compromis par l'attaquant et servir de moyens de persistance.

Ces différents éléments, composant le cœur de confiance du SI, doivent faire l'objet d'un plan d'action adapté selon la connaissance de l'attaque apportée par les investigations numériques.

Azure AD peut-il aider lors de la reconstruction?

Certainement, en mettant en service des solutions SaaS pour rétablir certains services de productivité.

Néanmoins, Azure AD ne sera pas utile dans les cas suivants :

- La grande majorité des applications utilisées dans les organisations sont liées à l'AD. Les autorisations sont généralement attribuées sur des comptes basés sur l'Active Directory *on-premises* et les applications ne savent même pas ce qu'est Azure AD
- Les organisations ne peuvent joindre (nativement) que les postes de travail (Windows 10/Windows 11) à Azure AD mais pas les serveurs

C'est pourquoi, il reste essentiel d'avoir une sauvegarde régulière et déconnectée d'Active Directory, pour être en mesure d'être résilient après une attaque de type ransomware.

FOCUS

Préparer la reconstruction de l'Active Directory

Incontournables

Sauvegarde de l'AD résiliente aux scénarios de cyberattaques retenus **et protégée**
Windows backup chiffré et hébergé sur un espace immuable

Accéder au SI sans dépendances à l'AD
Poste d'administration sain, by-pass du NAC, VPN sans AD

Environnement de confiance pour reconstruire
Infrastructure et réseau indépendants

Savoir mobiliser les bonnes personnes
Équipes d'audit, de réponse à incidents, de gestion de crise, opérationnelles

Recommandés

Disposer de procédures d'assainissement et de reconstruction de l'Active Directory
Formaliser, automatiser et s'entrainer

Accéder aux applications du SI sans Active Directory
Azure AD standalone pour Office 365, comptes locaux

À étudier

Anticiper l'opportunité de s'appuyer sur Azure AD pour reconstruire
Poste de travail en Azure AD join

Ne pas se contenter d'une simple reconstruction de l'AD

La reconstruction d'un SI suite à une Cyberattaque est un sprint nécessitant la mobilisation de tous. Le risque est cependant de penser que la course s'arrête là.
Dans ce cas, il n'est pas rare de subir quelques mois ou années après une nouvelle attaque.

« 80% des Entreprises ayant payées une rançon subissent une seconde Cyberattaque »
Cybereason

Ne pas se limiter à la crise mais transformer le SI

La reconstruction du SI permet de faire face au plus urgent et de passer un premier palier en terme de sécurité. La compromission du SI est, cependant, bien souvent, le symptôme d'une dette sécurité de plusieurs années. Il ne sera, par exemple, pas possible pendant la gestion de crise de quelques semaines, de transformer son modèle de sécurité ni de traiter toutes les obsolescences : le chemin de crête doit être défini pour rendre au plus vite le service au Métier.

La gestion de la crise doit être vue comme la première partie de la course permettant à l'entreprise de passer un cap en terme de maturité sécurité. Il est alors nécessaire de définir un programme de transformation du SI pour traiter la dette et bien souvent changer de modèle de sécurité pour le réaligner avec les besoins du métier : un vrai marathon !

« Un programme sur plusieurs années est nécessaire pour transformer son modèle de sécurité »

Conclusion

La sécurité des référentiels d'identité est souvent abordée avec de nombreux détails techniques, où les experts parlent aux experts.

Pour autant, il est possible de garder une approche pragmatique en se posant les bonnes questions : Comment est administré l'Active Directory ? Depuis quels postes de travail ? Les services ayant une relation forte avec ces serveurs, ces postes de travail sont-ils bien sécurisés ? La vision doit être élargie et prendre en compte dorénavant la sécurité d'Azure AD, qui n'est pas une simple extension d'Active Directory dans le *cloud*.

Il est nécessaire de définir une cible (court et moyen terme), en cohérence avec la stratégie de transformation de l'organisation.

La sécurité est une question d'arbitrage, il est primordial de connaître les vulnérabilités qui exposent l'organisation tout en ayant conscience du risque et des bénéfices associés. Cela aide à mieux décider de sa trajectoire de modernisation et de ses priorités.

Le modèle d'administration évolue et prend en compte les nouvelles dimensions de l'entreprise étendue à travers ces aspects hybride et *multi-cloud*.

Tout au long de cette transformation, les organisations devront rester concentrées sur l'essentiel, avec l'identité comme pierre angulaire de la sécurité des systèmes d'information.

Le système d'identité des organisations est dorénavant hybride et cette nouvelle réalité doit être embrassée.

Remerciements

AUTEURS

THOMAS DIOT
Senior Consultant,
Wavestone

THIBAULT JOUBERT
Manager,
Wavestone

ARNAUD JUMELET
National Security Officer,
Microsoft France

ÉTIENNE LAFORE
Senior Manager,
Wavestone

ALEXANDRE LUKAT
Manager,
Wavestone

CONTRIBUTEURS

PIERRE AUDONNET
Principal Customer Engineer,
Microsoft Canada

FLORENT BENOIT
Partner Technology Strategist,
Microsoft France

RÉMI ESCOURROU
Manager, Wavestone

JEAN-YVES GRASSET
Chief Security Advisor, Microsoft
France

BENOÎT MARION
Senior Manager, Wavestone

GREGORY SCHIRO
Compromise Recovery Security
Practice, Microsoft

JULIEN ROUSSON
Manager, Wavestone

Liens utiles

ANSSI - ACTIVE DIRECTORY CONTROL PATHS
https://github.com/ANSSI-FR/AD-control-paths

ANSSI - LE SERVICE ACTIVE DIRECTORY SECURITY (ADS)
https://www.ssi.gouv.fr/administration/actualite/le-service-active-directory-security-ads-accompagner-la-securisation-des-annuaires-active-directory-des-acteurs-critiques/

ANSSI - POINTS DE CONTRÔLE ACTIVE DIRECTORY
https://www.cert.ssi.gouv.fr/uploads/guide-ad.html

ANSSI - RECOMMANDATIONS DE SÉCURITÉ RELATIVES À ACTIVE DIRECTORY
https://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-a-active-directory

M365INTERNALS - INCIDENT RESPONSE IN A MICROSOFT CLOUD ENVIRONMENT (HUY KHA)
https://m365internals.com/2021/04/17/incident-response-in-a-microsoft-Cloud-environment/

MICROSOFT - APPENDIX L: EVENTS TO MONITOR
https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/appendix-l--events-to-monitor

MICROSOFT - AZURE ACTIVE DIRECTORY SECURITY OPERATIONS GUIDE
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/security-operations-introduction

MICROSOFT - BEST PRACTICES FOR AZURE AD ROLES
https://docs.microsoft.com/en-us/azure/active-directory/roles/best-practices

MICROSOFT – DÉTAILS DES LICENCES AZURE AD
https://www.microsoft.com/en-us/security/business/identity-access-management/azure-ad-pricing

MICROSOFT - ENTERPRISE ACCESS MODEL
https://docs.microsoft.com/en-us/security/compass/privileged-access-access-model

MICROSOFT - SECURING AZURE ENVIRONMENTS WITH AZURE ACTIVE DIRECTORY
https://aka.ms/AzureADSecuredAzure

MICROSOFT – OBJETS D'APPLICATION ET PRINCIPAL de SERVICE
https://docs.microsoft.com/en-us/azure/active-directory/develop/app-objects-and-service-principals

MICROSOFT - AZURE DEFENSES FOR RANSOMWARE ATTACK
https://azure.microsoft.com/en-us/resources/azure-defenses-for-ransomware-attack/

MICROSOFT – QU'EST-CE QU'IDENTITY SECURE SCORE ?
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/identity-secure-score

MICROSOFT – SECURISATION DES COMPTES DE SERVICE AZURE
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/service-accounts-introduction-azure

MICROSOFT – DOCUMENTATION SUR LES IDENTITES EXTERNES
https://docs.microsoft.com/fr-fr/azure/active-directory/external-identities/

MICROSOFT – MICROSOFT AZURE AD ASSESSMENT
https://github.com/AzureAD/AzureADAssessment

Microsoft s'engage en faveur d'un numérique de confiance, inclusif et durable. Sa mission est de donner à chaque individu et chaque organisation les moyens de réaliser ses ambitions, à l'ère du Cloud intelligent et de l'*intelligent edge*.

Catalyseur de l'innovation dans l'Hexagone depuis près de 40 ans, Microsoft France est présidée par Corine de Bilbao depuis juillet 2021. Avec plus de 1 800 collaborateurs et 10 500 partenaires économiques, technologiques, acteurs du secteur public, chercheurs ou start-ups, Microsoft France contribue au développement de l'économie et des compétences numériques sur l'ensemble du territoire français

Dans un monde où savoir se transformer est la clé du succès, Wavestone s'est donné pour mission d'éclairer et guider les grandes entreprises et organisations dans leurs transformations les plus critiques avec l'ambition de les rendre positives pour toutes les parties prenantes. C'est ce que nous appelons « The Positive Way ».

Parmi les leaders indépendants du conseil en Europe, Wavestone rassemble plus de 3 000 collaborateurs dans 8 pays dont plus de 600 consultants en cybersécurité. Ces derniers accompagnent des organisations sur tous les enjeux de cybersécurité, des plus stratégiques à la mise en œuvre opérationnelle, en passant par la réponse à incident et l'investigation numérique.
Wavestone est coté sur Euronext à Paris.

Plus d'informations sur www.wavestone.com/fr/
@Wavestone_
@RiskInsight

The Positive Way

WAVESTONE

www.microsoft.com

www.wavestone.com