semperis

Votre plan de reprise après sinistre pour Active Directory tient-il compte des cyberattaques ?

PAR GUIDO GRILLENMEIER ET GIL KIRKPATRICK

RÉCUPÉRATION D'ACTIVE DIRECTORY DANS LE CONTEXTE DES MENACES ACTUELLES

Il y a seize ans, Gil Kirkpatrick – Architecte en chef chez Semperis – et Guido Grillenmeie – Technologue en chef chez Semperis – (qui travaillaient tous les deux dans d'autres entreprises à l'époque) se sont associés pour partager leur expérience et leur expertise en matière de protection et de récupération d'Active Directory (AD). Fruit de cette collaboration : la publication en 2005 du livre blanc « A Definitive Guide to Active Directory Disaster Recovery ». Ce livre blanc répondait à un besoin crucial du secteur, car les entreprises avaient pour la plupart accepté AD comme le service d'annuaire par défaut à utiliser pour contrôler l'accès de leurs utilisateurs au réseau, aux applications et aux services de l'entreprise.

À ce moment-là, les informations sur la récupération de tout ou partie du service AD étaient rares, et peu de spécialistes AD comprenaient la nature du défi à relever. Ce livre blanc explique les mécanismes de la récupération AD et précise la nécessité, pour les entreprises, de se préparer à une récupération adéquate en cas de problèmes liés à AD. Il décrit les méthodes de récupération après plusieurs types de sinistres, notamment la suppression par inadvertance d'objets AD, les erreurs de configuration des stratégies de groupe et les pannes de contrôleurs de domaine AD. Le document se termine par une brève description du processus de récupération d'un environnement AD après une défaillance globale, avec une remarque : « La probabilité qu'une restauration complète de la forêt AD soit nécessaire est toutefois minime ».

Mais ça, c'était avant. Désormais, le panorama de la cybersécurité a changé radicalement. Il ne se passe pas une semaine sans que le réseau Windows sur site d'une entreprise ne soit dévasté par une attaque de type ransomware ou wiper. Par exemple, entre 2019 et début 2020 (avec estimation des coûts de récupération) :

- Ville de la Nouvelle-Orléans (plus de 3 millions de $)
- Ville de Baltimore (18 millions de $)
- Norsk Hydro (70 millions de $)
- Demant (80 millions de $)

Et ce n'est que quelques exemples parmi des dizaines d'autres. En fait, la possibilité de récupérer votre environnement AD dans son intégralité à partir d'une sauvegarde n'est plus une réponse intéressante face à un événement hautement improbable. C'est une obligation.

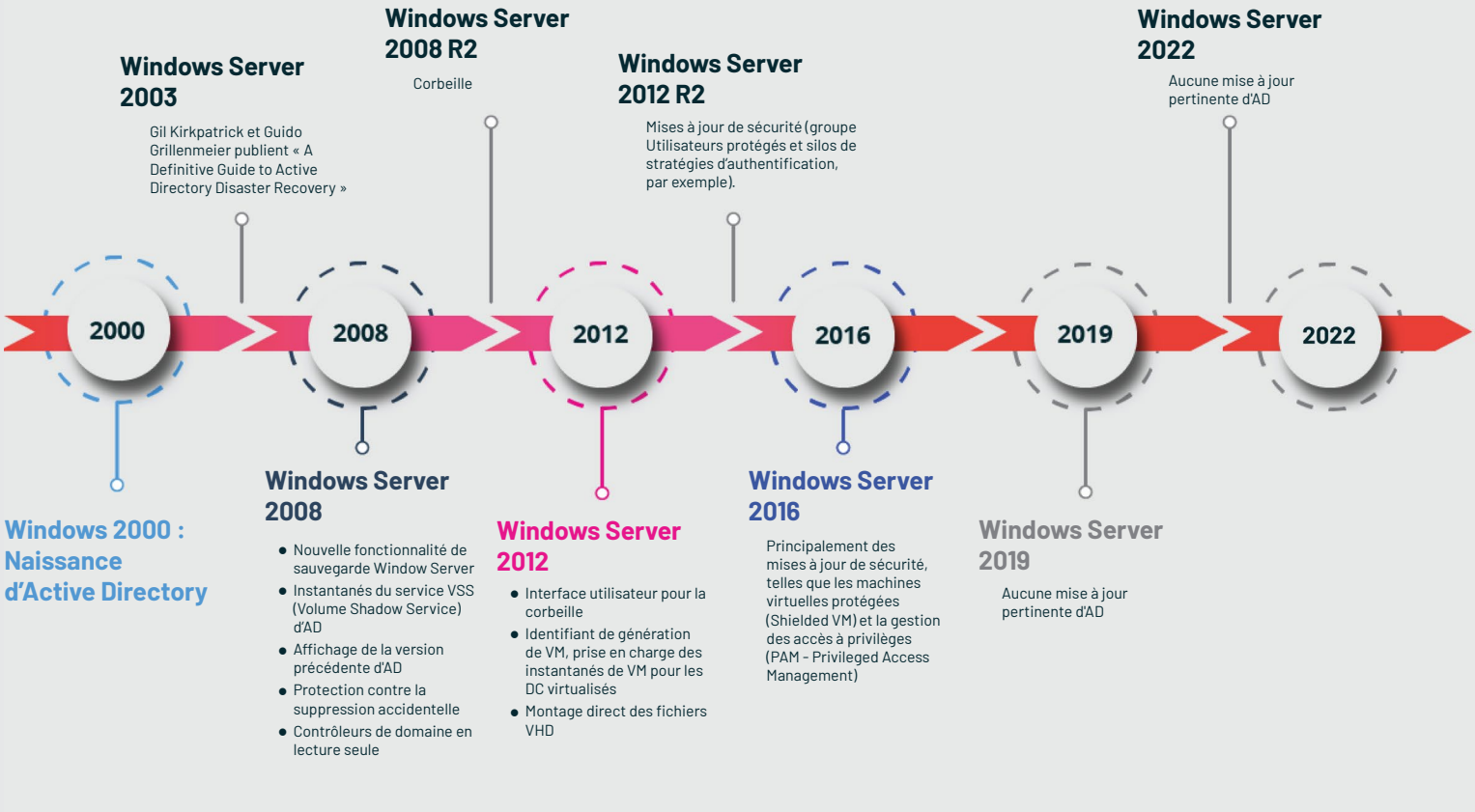
Le système d'exploitation Windows Server et son service Active Directory intégré ont évolué de façon radicale depuis 2005, au même titre que le modèle de menace. Microsoft a nettement amélioré la sécurité de Windows, ajouté des fonctions et des capacités permettant de simplifier la récupération des objets AD, et perfectionné le comportement d'AD en environnement virtualisé. Mais les problèmes fondamentaux liés à la récupération d'une forêt Active Directory complète à partir d'une sauvegarde n'ont pas évolué. Cela reste un processus complexe, source d'erreurs, qui nécessite une planification et de la pratique pour la quasi-totalité des déploiements AD, à l'exception des plus simples.

Il est intéressant de noter que les deux dernières versions de Windows Server (Windows Server 2019 et 2022) sont les premières versions de Windows Server sans mise à jour du service AD lui-même. Apparemment, selon Microsoft, il n'y a plus de problèmes à résoudre dans AD et aucune autre amélioration du service n'est nécessaire. Qui plus est, la reprise après sinistre d'AD ne va pas aller en s'améliorant.

Nous devons maintenant évaluer les capacités de récupération d'une entreprise en la replaçant dans le contexte des nouvelles cybermenaces qui visent AD de nos jours, et dont nous n'avions pas à nous préoccuper en 2005. Malheureusement, l'augmentation du nombre d'attaques signifie que les entreprises doivent se préparer de toute urgence à une récupération rapide en cas d'attaque contre leur AD. Les perfectionnements dont Microsoft a fait preuve au cœur du service AD au fil des ans peuvent toutefois se révéler d'un faible secours pour la récupération de votre AD en cas d'attaque. Votre entreprise est-elle prête à récupérer rapidement son AD d'entreprise en cas de sinistre réel qui anéantirait l'ensemble du service ?

« Les entreprises doivent se préparer de toute urgence à une récupération rapide en cas d'attaque contre leur AD ».

Changements liés à la sauvegarde d'Active Directory au fil du temps



Votre entreprise est-elle prête à récupérer rapidement son AD d'entreprise en cas de sinistre réel qui anéantirait l'ensemble du service ?

POURQUOI LA PROTECTION D'ACTIVE DIRECTORY EST SI IMPORTANTE

Active Directory (AD) est en production depuis plus de 20 ans. Dans sa conception initiale, ce rôle de serveur Microsoft offre les fonctionnalités suivantes :

Authentification : Authentifie les utilisateurs sur site qui se connectent à leur PC et au réseau de l'entreprise, ainsi que les utilisateurs distants qui se connectent à des applications hébergées en interne ou à des postes de travail virtuels

Autorisation : Contrôle les ressources intégrées à AD (services de fichiers, impression, Exchange Server, SharePoint Server et SQL Server, par exemple) auxquelles ils ont le droit d'accéder

Sécurité et contrôle : La politique du groupe peut appliquer des configurations de politique à chaque ordinateur, serveur et utilisateur rattaché à AD

Annuaire : Emplacement unique permettant de trouver des utilisateurs et des ressources

DNS : DNS intégré à AD pour assurer la résolution des noms de réseau

PKI : Les services Active Directory Certificate fournissent des certificats aux utilisateurs et aux ordinateurs du domaine

La popularité croissante du système d'exploitation Windows Server, qui offre des services de base en matière de partage de fichiers et d'impression (ainsi que des services de back-office tels qu'e-mail, messagerie et outils de collaboration), a contribué à faire d'AD la référence en matière d'annuaire réseau. Microsoft a fait évoluer la quasi-totalité de ses applications classiques pour qu'elles en dépendent, faisant d'AD l'un des services logiciels les plus utilisés dans les entreprises actuelles. À l'échelle mondiale, plus de 90 % des entreprises comptant plus de 500 employés utilisent AD.

L'essor du cloud computing ne change rien à cette situation. Il a même accru l'importance d'AD pour l'entreprise. Deux facteurs expliquent l'importance d'AD au sein du cloud.

Tout d'abord, le modèle de cloud computing ne dépend pas de réseaux de confiance comme c'est le cas pour l'informatique traditionnelle sur site car, contrairement aux réseaux d'entreprise traditionnels, le trafic entre les clients et les ressources accessibles se fait le plus souvent via le réseau Internet public. Ce trafic n'est pas sécurisé en fonction de OÙ vous êtes, mais en fonction de QUI vous êtes. Comme le souligne Microsoft, « l'identité est le plan de contrôle » par lequel l'accès aux ressources du cloud est contrôlé. L'identité d'un utilisateur est au cœur de la sécurité du cloud.

Ensuite, AD constitue la base de l'architecture d'identité hybride couramment utilisée à l'heure actuelle. Dans ce type d'architecture, les entreprises synchronisent leur magasin de données d'identité sur site (généralement AD) avec le service cloud de gestion des identités de leur choix, tel qu'Azure Active Directory, Okta ou Amazon Web Services (AWS). Cette approche permet aux utilisateurs d'utiliser leur identité professionnelle pour accéder aux ressources (Office 365 ou Salesforce, par exemple) intégrées au service cloud de gestion des identités de l'entreprise.

Qui plus est, de nombreuses entreprises n'accordent pas la même confiance aux services cloud qu'à leurs systèmes contrôlés en interne, qui sont entièrement gérés par leur propre personnel informatique. C'est pourquoi beaucoup ont décidé de mettre en place un cadre d'authentification fédérée en utilisant AD Federation Services (ADFS) (ou des solutions similaires) pour se connecter aux solutions cloud. C'est le cas par exemple d'Azure AD. Dans ce cas, la validation de l'identité de l'utilisateur (c'est-à-dire son authentification) continue de se faire sur la base de son AD sur site. ADFS crée ensuite un jeton spécifique, le jeton SAML, qui confirme au service cloud (Azure AD et les applications associées, par exemple) que l'utilisateur qui se connecte est bien celui qu'il prétend être. Étant donné que le jeton SAML est correctement crypté au moyen d'une clé partagée entre ADFS et Azure AD uniquement, Azure AD fait totalement confiance à ce jeton et autorise l'utilisateur à accéder aux ressources cloud correspondantes. En substance, Azure AD fait entièrement confiance à votre AD sur site dans cette configuration.

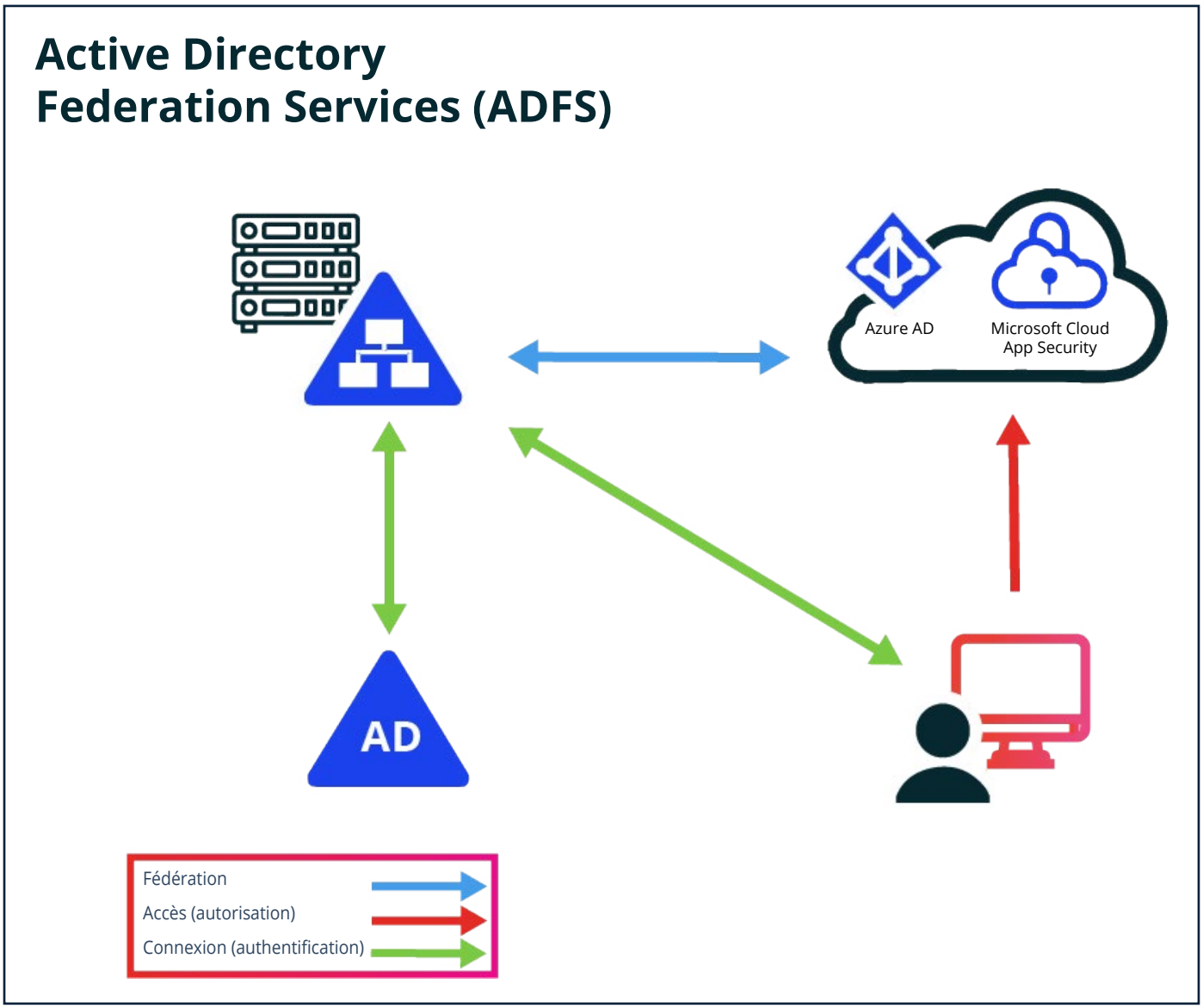


Figure 1 : La fédération s'appuie généralement sur votre AD sur site pour certifier l'identité de vos utilisateurs

S'ajoute à cela le fait que, malgré tout le battage médiatique et le passage au cloud computing, toutes les entreprises, quelle que soit leur taille ou leur ancienneté, mènent des opérations sur site importantes et constantes qui dépendent d'AD. Par conséquent, AD reste de nos jours incontournable pour avoir accès aux ressources sur site, mais constitue aussi un élément essentiel de l'entreprise hybride d'aujourd'hui et de toutes ses applications.

ÉVOLUTION DU PANORAMA DES MENACES

Lorsque le document intitulé « Definitive Guide to Active Directory Disaster Recovery » a été rédigé, les principaux sinistres que les administrateurs AD devaient craindre se classaient dans deux catégories : les sinistres physiques (panne de courant, crash de disque ou inondation, par exemple) et les erreurs administratives (involontaires ou malveillantes) qui entraînent la modification ou la suppression inappropriée d'objets AD. Une troisième catégorie (la défaillance d'un service à l'échelle de la forêt) est intéressante en théorie, mais elle a très rarement eu lieu dans la réalité. Les conséquences d'une défaillance totale de la forêt étaient certes désastreuses, mais elles étaient si improbables que la plupart des entreprises acceptaient le risque résiduel correspondant.

En 2021, cette évaluation des risques a été complètement chamboulée. AD conserve une bonne gestion des problèmes liés aux serveurs physiques et aux sites, et après 10 à 20 ans d'expérience, la plupart des entreprises peuvent administrer leur Active Directory de manière fiable et sûre. Mais les cybercriminels, équipés d'outils de phishing sophistiqués et des derniers logiciels malveillants en matière de reconnaissance, de persistance et de cryptage de données, peuvent anéantir tout un environnement Windows d'entreprise en quelques minutes. Les dernières statistiques portant sur les ransomwares font froid dans le dos.

En 2020 :

51 % des entreprises ont été touchées par une attaque de type ransomware. (PentTst Magazine)

Les ransomwares coûtent aux entreprises environ 75 milliards de $ par an (Datto)

La rançon moyenne demandée est de 178 000 $ et le paiement le plus important rendu public est de 11,8 millions de $

La perte de l'intégralité du service Active Directory est passée du bas de l'échelle des risques au sommet.

Active Directory est une cible de choix pour les cybercriminels

Active Directory a été conçu pour faire face aux catastrophes physiques. Si un DC tombe en panne, voire si tout un centre de données s'arrête, AD continuera à fonctionner avec les contrôleurs de domaine restants. Microsoft a ajouté la fonction de corbeille AD dans Windows Server 2008 R2, qui permet de récupérer de manière satisfaisante les objets supprimés accidentellement. Quant à la possibilité d'annuler les modifications apportées par inadvertance aux objets AD, vous ne pouvez compter que sur vous-même.

Il est clair que le service AD est un service de base indispensable dans presque toutes les entreprises. AD stocke les informations d'identification des utilisateurs, des ordinateurs et des services, et contrôle l'authentification et l'autorisation à travers l'ensemble de l'environnement sur site. Cela fait d'AD une cible de choix pour les auteurs de menaces, pour trois raisons :

- En tant que service d'annuaire, AD est un point d'accès unique aux informations dont les auteurs de menaces ont besoin pour progresser latéralement sur le réseau et accroître leurs privilèges.
- En tant que principal service d'authentification et d'autorisation, AD est un point d'attaque qui peut rendre le reste du réseau inutilisable.
- AD, qui est de facto la solution de gestion de la configuration des postes via la stratégie de groupe, est un outil supplémentaire que les attaquants peuvent utiliser pour distribuer des logiciels malveillants et les rendre persistants sur plusieurs machines du réseau.

Alors que nous n'entendons généralement jamais parler des détails techniques dans les articles consacrés aux cyberattaques, nous commençons à voir Active Directory mentionné beaucoup plus régulièrement :

- L'Active Directory de Virgin Mobile a été piraté et ses données vendues sur le Dark Web.
- NTT Communication a admis que son Active Directory avait été piraté dans le cadre d'une violation de données.
- Il a été démontré que le ransomware Ryuk modifiait la stratégie de groupe pour se propager jusqu'aux postes de travail via un script de connexion.

Pour tout dire, nous avons toujours été capables de retracer la ligne pointillée, sachant qu'Active Directory risquait fort de faire partie d'une attaque ; nous avons maintenant des données pour le prouver.

POURQUOI ACTIVE DIRECTORY EST VULNÉRABLE

Active Directory fonctionne très bien, son concept a résisté à l'épreuve du temps. Cependant, le monde a changé tout autour, avec l'émergence des versions cryptées, l'ouverture aux requêtes, Kerberos, et la sophistication croissante des attaques recourant à des outils tels que Mimikatz.

APT (Advanced Persistent Threat) : Infiltration et violation

Les attaques contre AD ont connu une augmentation spectaculaire au cours des dernières années, car les pirates ont compris que s'ils possédaient AD, ils possédaient les ressources informatiques de l'entreprise. C'est un lieu commun que d'affirmer qu'AD « détient les clés du royaume », mais même cette formule sous-estime le risque : ce service détient également une véritable « carte au trésor » permettant d'accéder à toutes les ressources AD intégrées de l'entreprise. Les utilisateurs finaux ne sont pas conscients de leur dépendance à l'égard d'AD, mais les outils et les processus opérationnels qu'ils utilisent tous les jours risquent de ne pas fonctionner si AD ne fonctionne pas. Cela inclut les applications liées à des services essentiels tels que la messagerie électronique (Exchange), le partage de fichiers (SharePoint, partages de fichiers normaux), la collaboration (Skype) ou même la fonction d'impression. De nombreuses entreprises utilisent par ailleurs l'authentification intégrée à Windows pour bon nombre de leurs applications et bases de données opérationnelles, où « intégrée à Windows » est simplement un autre terme pour « intégrée à AD », c'est-à-dire que les applications ne s'appuient pas sur leur propre liste d'utilisateurs, mais « font confiance » au jeton d'accès d'un utilisateur généré par AD pour octroyer un accès approprié à l'application. AD ne contrôle pas seulement l'accès à ces applications par les utilisateurs légitimes : il permet également aux pirates de comprendre quelles applications ont été intégrées à une infrastructure et donc de les utiliser contre vous.

À mesure que l'on reconnaît que le service AD est une cible de choix, les outils pour l'attaquer se multiplient. PowerSploit, Bloodhound, Death Star, Cobalt Strike et surtout Mimikatz ont permis aux pirates de trouver rapidement des informations d'identification, de procéder à une reconnaissance horizontale du réseau, de trouver le chemin le plus court vers les droits d'administration du domaine et de cibler ce chemin d'accès.

Ces outils permettent de dominer un domaine en quelques heures au lieu de plusieurs jours. Par conséquent, il est désormais plus facile que jamais de mener à bien une attaque contre Active Directory.

Le cybersinistre : Attaques DoA

AD est étonnamment tolérant aux pannes en cas de sinistre physique ou de catastrophe naturelle. Ouragans, tornades, tremblements de terre, pannes de courant et autres événements qui mettent hors service un centre de données affecteront localement un service AD bien conçu, tout en permettant au reste du réseau de continuer à utiliser le service. Une fois la section paralysée du service AD rétablie, tous les changements survenus au sein du réseau pendant la période de défaillance seront automatiquement transférés dans cette section. Un incident qui détruirait l'ensemble d'un domaine ou d'une forêt AD aurait un impact très important, mais serait également rarissime en raison des précautions prises par les entreprises pour répartir géographiquement leurs infrastructures AD. C'est pourquoi le risque d'indisponibilité totale d'AD n'a jamais été classé comme supérieur à modéré. Ajoutez à cela le coût élevé de la continuité des activités et de la reprise après sinistre (BCDR) d'Active Directory (nous y reviendrons plus tard) et vous comprendrez que la planification BCDR a toujours négligé la reprise des forêts.

Les attaques DoA (denial-of-availability) Les variantes les plus connues de cette catégorie sont les ransomwares et les wiperwares Nous savons tous ce qu'est un ransomware. Quasiment tous les jours, on apprend que les clients, les serveurs et les données d'une entreprise ont été piratés et que les pirates exigent une certaine somme en bitcoins pour obtenir la clé de décryptage. Les wiperwares détruisent vos ordinateurs et vos données, que ce soit par le biais du cryptage ou de la suppression pure et simple des données, sans possibilité de récupération.

L'attaque NotPetya de 2017 en est l'exemple le plus connu à ce jour. La compagnie de transport maritime par conteneurs Maersk a été l'une des principales victimes. NotPetya a anéanti des milliers d'ordinateurs, de serveurs et, en fait, tous les contrôleurs de domaine AD de Maersk au niveau mondial, y compris leurs sauvegardes. Ils ont simplement eu la chance qu'une panne de courant empêche le malware de se propager jusqu'au contrôleur de domaine de leur site au Ghana : ils ont finalement pu utiliser ce DC pour la récupération de leur AD. Après avoir fait l'objet d'une reprise très coûteuse, estimée entre 250 et 300 millions de $, Maersk a décidé de parler publiquement de sa situation pour sensibiliser d'autres entreprises aux risques d'attaque de leur infrastructure par les logiciels malveillants modernes. Les entreprises doivent se préparer à cette menace, car la plupart d'entre elles ne survivraient pas à une panne de neuf jours de leur système informatique central ; or, c'est précisément le temps qu'il a fallu à Maersk pour récupérer complètement son Active Directory.

FedEx, Saint-Gobain, Reckitt Benckiser et Mondelēz comptent parmi les autres victimes lourdement touchées par l'attaque NotPetya. Et l'attaque NotPetya est loin d'être la dernière attaque contre AD. Elle ne représente que le début d'une nouvelle ère d'attaques par ransomware à propagation rapide qui utilisent et affectent Active Directory. Malheureusement, les vecteurs d'attaque contre AD sont nombreux : il y a peu, une attaque menée avec succès par Nefilim a réussi à utiliser le compte d'administrateur de domaine d'un employé décédé, qui jouissait de nombreux droits d'accès, pour ouvrir toutes les portes aux pirates.

Vos sauvegardes Active Directory ne vous aideront pas à récupérer votre service AD

Dans le cas d'un cybersinistre, les sauvegardes normales d'Active Directory ne vous aideront pas à reprendre vos activités opérationnelles suite à l'attaque. La fonction de protection des objets contre les suppressions accidentelles permet d'éviter les erreurs humaines, mais ne résout pas le problème des activités malveillantes au sein de votre AD.

Il en va de même pour la corbeille, qui permet de récupérer les objets supprimés, mais pas d'annuler les modifications apportées au niveau des attributs, ni les modifications apportées aux GPO ou à la configuration de votre AD. La corbeille ne peut pas non plus vous aider à récupérer l'ensemble de votre domaine ou de votre forêt, ainsi que les partitions d'applications associées

L'utilisation d'instantanés peut permettre de déceler les modifications apportées aux attributs et de les annuler, mais elle ajoute une grande complexité au processus de récupération.

Aucune de ces méthodes de restauration des données d'Active Directory ne suffira pour vous aider à récupérer le service AD réel, c'est-à-dire l'intégralité de votre domaine ou de votre forêt. Nous espérons tous ne jamais en avoir besoin, mais une corruption de schéma due à une modification malveillante opérée par un pirate, ou encore le cryptage de tous vos DC par un logiciel malveillant peuvent nécessiter une récupération de votre AD au niveau de la forêt. Pour cela, il est nécessaire d'effectuer une sauvegarde correcte des DC AD.

Préparation d'une sauvegarde qui permette une récupération du service Active Directory sans logiciel malveillant

La récupération du service Active Directory, c'est-à-dire la récupération du fichier NTDS.dit et des fichiers et paramètres du système d'exploitation associés pour pouvoir répliquer correctement les données AD, est une tâche beaucoup plus difficile que la simple récupération d'objets AD spécifiques. Si toutes les modifications apportées à tous les objets et attributs étaient conservées sur un seul serveur de base de données AD (un seul contrôleur de domaine), la récupération du serveur serait simple, et correspondrait à celle d'un serveur de fichiers.

Mais la grande force et le succès d'Active Directory reposent justement sur sa capacité à ne pas limiter les modifications effectuées dans l'annuaire à un seul serveur ou à un seul master, contrairement à ses prédécesseurs. AD a plutôt été conçu comme une architecture de base de données multimaster, ce qui permet d'effectuer des changements sur n'importe quel contrôleur de domaine (accessible en écriture) au sein du réseau d'une entreprise. C'est ce qui a permis d'assurer l'extensibilité et la répartition géographique du service Active Directory et de faire en sorte qu'un domaine ou une forêt AD puisse desservir de nombreux sites répartis dans le monde entier.

Nous abordons les points précis de la sauvegarde globale des DC de façon plus détaillée dans le « Definitive Guide » mais il est tout aussi important de réfléchir à la répartition géographique de vos DC AD et de leurs sauvegardes que d'effectuer la sauvegarde elle-même. Pendant la planification de votre sauvegarde AD, vous devez à tout moment vous demander si les sauvegardes DC choisies sont suffisantes pour récupérer rapidement votre forêt AD. Cette opération est particulièrement difficile dans une forêt multidomaines, c'est-à-dire une forêt qui compte plusieurs domaines enfant ou arbres parallèles qui font partie de la même structure de forêt AD. Dès que votre forêt AD contient plusieurs domaines, le catalogue global est une fonctionnalité AD nécessaire qui devra être reconstruite et réactivée lors d'un processus de récupération de la forêt, avant de pouvoir redémarrer les services d'authentification. Et la reconstruction de ce catalogue global prendra beaucoup plus de temps si au moins un DC de chaque domaine de votre forêt n'est pas situé sur le même site AD. Un peu plus loin, nous abordons d'autres difficultés liées à la récupération rapide de votre forêt.

Intégration à Volume Shadow Copy Service

Il va sans dire que l'outil de sauvegarde utilisé pour sauvegarder vos DC Active Directory doit intégrer la fonction Volume Shadow Copy Service (VSS) du système d'exploitation Windows Server. Cette intégration garantit un état cohérent de votre base de données AD au moment de l'exécution d'une sauvegarde – par exemple, toutes les opérations d'écriture en cours seront terminées et écrites sur le disque, tandis que les nouvelles modifications apportées à la base de données AD sont arrêtées au moment où un instantané de la base de données AD est effectué. Ce processus ne prend que quelques secondes ; l'outil de sauvegarde dispose ensuite de tout le temps nécessaire pour copier l'état cohérent de la base de données AD sur la cible de votre choix, tandis que les opérations d'écriture sur la base de données AD d'origine peuvent continuer à faire fonctionner le contrôleur de domaine AD comme d'habitude.

L'outil intégré WBS (Windows Server Backup) est un bon exemple d'outil de sauvegarde entièrement intégré à VSS, qui vous permettra d'effectuer deux types de sauvegardes :

1. SSB (System State Backup – sauvegarde de l'état du système)
2. BMR (Bare Metal Restore/Recovery – restauration/ récupération à chaud).

Ces deux options sont très différentes en termes de cas d'utilisation : soyez donc attentif aux différentes fonctionnalités lorsque vous planifiez votre stratégie de sauvegarde.

Les sauvegardes de l'état du système peuvent contenir des logiciels malveillants

L'option de sauvegarde de l'état du système permet de sauvegarder tous les éléments critiques du système d'exploitation du serveur d'un DC (notamment la base de données AD (NTDS.dit), le dossier SYSVOL, la base de données d'enregistrement des classes COM+, le registre du serveur et les fichiers de démarrage), tout en évitant les données utilisateur, les disques supplémentaires et les données susceptibles d'avoir été ajoutées pour d'autres applications fonctionnant sur le même serveur. Même si la sauvegarde utilise les capacités VSS pour créer un instantané fidèle des disques utilisés par le serveur, le transfert de la sauvegarde réelle de l'état du système est constitué d'une copie des fichiers pertinents sur la cible de sauvegarde, ce qui ne permet pas d'effectuer des sauvegardes incrémentielles, c'est-à-dire que vous devez dans tous les cas transférer l'état complet du système vers l'emplacement de sauvegarde cible. Une sauvegarde de l'état du système stocke, en plus de votre base de données AD, environ 11 Go de fichiers du système d'exploitation Windows lors de chaque sauvegarde de DC.

La restauration de la sauvegarde de l'état du système doit être effectuée sur la même instance de Windows Server et la même installation de système d'exploitation que celles qui ont servi à sa création, ce qui signifie qu'elle a pour but de contribuer à la résolution d'un problème au niveau du système d'exploitation ou des données, mais pas à la résolution d'un problème matériel impliquant la reconstruction intégrale du serveur. Par conséquent, une sauvegarde de l'état du système peut être utilisée pour la récupération de la base de données AD si vous devez restaurer des éléments d'une base de données AD afin de récupérer de manière autorisée des objets supprimés accidentellement d'AD. Par contre, une sauvegarde de l'état du système ne vous aidera pas à récupérer votre sauvegarde sur un serveur récemment déployé (et encore moins sur un serveur dont le matériel est différent ou dont l'architecture passe du physique au virtuel, ou vice versa). Bien sûr, la sauvegarde de l'état du système peut être la seule solution si, après une cyberattaque, vous avez besoin de récupérer rapidement vos DC AD sur d'autres équipements ou machines virtuelles qui seront peut-être disponibles plus vite. Dans tous les cas, gardez à l'esprit que la sauvegarde de l'état du système englobe certains fichiers du système d'exploitation qui ont été sauvegardés : il est donc très probable qu'une nouvelle infection ait lieu à partir d'un logiciel malveillant sauvegardé avec AD.

« Gardez à l'esprit que la sauvegarde de l'état du système englobe certains fichiers du système d'exploitation qui ont été sauvegardés : il est donc très probable qu'une nouvelle infection ait lieu à partir d'un logiciel malveillant sauvegardé avec AD ».

« A l'instar des sauvegardes de l'état du système, une certaine prudence est indispensable lors de la restauration d'AD à partir de sauvegardes BMR à la suite d'une cyberattaque, pour ne pas risquer de réintroduire des logiciels malveillants ».

Les sauvegardes BMR peuvent elles aussi contenir des logiciels malveillants

Comme leur nom l'indique, les sauvegardes créées avec l'option de reprise à chaud BMR (bare metal recovery), également appelées sauvegardes « full server », permettent de récupérer un serveur à l'état sauvegardé, en récupérant notamment le système d'exploitation et les services qui y sont exécutés, ainsi qu'Active Directory. L'objectif consiste à vous protéger contre les défaillances matérielles classiques (« disques cassés », par exemple). Mais dans le même temps, les sauvegardes BMR présentent le risque de réintroduire des logiciels malveillants si elles sont utilisées dans le cadre de la restauration d'AD.

L'option BMR permet de sauvegarder tous les disques utilisés par le système d'exploitation, ce qui comprend l'état du système. Vous pouvez aussi choisir de sauvegarder des disques supplémentaires sur le serveur correspondant. Une sauvegarde BMR est créée à l'aide de la méthode de sauvegarde centrée sur les blocs. Vous avez donc la possibilité de configurer des sauvegardes portant uniquement sur les blocs modifiés depuis la dernière sauvegarde : Vous pouvez exécuter une sauvegarde incrémentielle, pour accélérer encore un peu plus vos sauvegardes. Les sauvegardes incrémentielles fonctionnent si vous avez configuré l'option correspondante dans les paramètres de performance de sauvegarde sur votre serveur, et que votre disque de sauvegarde cible est hébergé sur le même serveur que celui que vous êtes en train de sauvegarder. Cette deuxième méthode peut sembler paradoxale, mais elle fonctionnera si vous possédez des dispositifs supplémentaires vous permettant de stocker ensuite les fichiers de sauvegarde créés sur une autre cible de stockage sécurisée.

Pendant la récupération, vous devez démarrer le serveur réparé à l'aide d'un disque d'installation Windows Server OS approprié, afin de le restaurer à partir du fichier de sauvegarde respectif. Notez que cette installation serveur doit aussi posséder le même type de matériel et d'architecture. Par exemple, l'option BMR ne permet pas de récupérer une sauvegarde de serveur Dell vers un nouveau serveur HPE, ni de choisir une machine virtuelle comme cible de récupération. Compte tenu de cette limitation (et du fait qu'il existe une option simple permettant de créer une nouvelle réplique de contrôleur de domaine AD en la faisant évoluer après une installation de système d'exploitation propre vers un matériel quelconque), la méthode BMR est peu utilisée pour effectuer des sauvegardes des DC Active Directory. Comme pour toute sauvegarde de l'état du système, les sauvegardes BMR sont exposées au même risque de présence de logiciels malveillants qui pourraient avoir infecté vos DC AD avant de devenir actifs et d'endommager votre forêt AD. A l'instar des sauvegardes de l'état du système, une certaine prudence est indispensable lors de la restauration d'AD à partir de sauvegardes BMR à la suite d'une cyberattaque, pour ne pas risquer de réintroduire des logiciels malveillants.

Sachez également que les sauvegardes SSB et BMR ne sont pas cryptées à l'aide de la fonction de sauvegarde Windows Server, ce qui signifie que vos sauvegardes sont vulnérables pendant leur transit et sûrement au repos, si vous n'avez pas crypté le disque sur lequel elles se trouvent. Cela implique également que vous ne devez pas copier les fichiers de sauvegarde sur un autre système de stockage cible accessible aux administrateurs de domaine non autorisés sans les avoir préalablement cryptés de manière appropriée.

Prenez soin de stocker les fichiers de sauvegarde de façon sécurisée, en vous assurant que seuls les administrateurs du service AD y ont accès.

Prudence avec les instantanés

Les instantanés sont néfastes ! Les instantanés à la rescousse !

Ces deux affirmations ont du sens. Jusqu'à la sortie de Windows Server 2012, qui a ajouté un identifiant spécifique pour la version d'une VM lors de l'utilisation d'instantanés (VMGenID3), Microsoft devait mettre en garde en permanence contre l'impossibilité de prendre des instantanés de DC au sein d'environnements virtuels. Les administrateurs risquaient en effet de commettre l'erreur de ramener un DC « en arrière » sans utiliser la méthode de récupération AD appropriée, qui consiste à informer les autres DC de l'environnement concerné de ce « retour en arrière ». Cette erreur peut occasionner toutes sortes de problèmes de réplication, car elle interrompt la logique de réplication intégrée à l'écosystème complexe d'AD. Une annulation du numéro de séquence de mise à jour (USN) peut se produire, et avec elle, un état d'objet non fiable dans la forêt AD, avec le risque de créer des SID en double et des objets persistants.

En partant du principe qu'actuellement tous vos DC fonctionnent au minimum sous Windows Server 2012 et que vous utilisez un hyperviseur prenant en charge la logique VMGenID (c'est le cas de tous les principaux hyperviseurs depuis quelques années maintenant), nous pouvons vous expliquer en détail pourquoi le retour à une version antérieure des DC via un instantané de VM n'est pas une bonne idée. Même s'il ne s'agit en aucun cas d'un mécanisme de sauvegarde de votre forêt AD, vous pouvez au moins éviter de nuire à AD en utilisant la technologie des instantanés VM.

Dans le livre blanc à paraître, « The New Definitive Guide to Active Directory Disaster Recovery », nous aborderons les principaux changements introduits par Microsoft avec Windows Server 2008, qui ont eu un impact sur la sauvegarde et la récupération AD en natif : L'intégration de la base de données AD aux capacités VSS du système d'exploitation. Nous aborderons aussi la nouvelle fonction WSB (Windows Server Backup), lancée avec Windows Server 2008 également, qui permet d'accéder aux données de sauvegarde sous forme de fichier VHD. Et nous détaillerons la fonctionnalité très pratique que Microsoft a introduite dans la version 2012 : la possibilité de monter des fichiers VHD directement sur un client Windows existant, afin de consulter rapidement une version antérieure de la base de données AD.

Grâce à tous ces changements, il est plus facile pour les administrateurs de récupérer des fichiers d'une version antérieure de votre dossier SYSVOL, par exemple, ou encore d'utiliser une version en lecture seule de vos données AD pour récupérer les attributs écrasés de l'un de vos objets. Pour combler les lacunes de sécurité d'Active Directory, il est primordial de protéger correctement vos fichiers de sauvegarde, car toute personne ayant accès à ces fichiers sensibles peut faire exactement ce que vous pouvez faire vous-même. Elle peut même utiliser d'autres outils de modification offline pour récupérer les hachages de mots de passe et autres données sensibles de la sauvegarde AD. Prenez soin de stocker les fichiers de sauvegarde de façon sécurisée, en vous assurant que seuls les administrateurs du service AD y ont accès.

Attention aux contraintes des outils de sauvegarde tiers

En fait, tout outil de sauvegarde qui se dit capable de sauvegarder AD actuellement devra également être intégré aux capacités VSS du système d'exploitation ou même utiliser la fonction WSB (Windows Server Backup) et y intégrer une intelligence supplémentaire permettant de sauvegarder de manière centralisée une sélection appropriée de vos DC.

Cependant, comme avec l'outil WSB intégré, être capable de sauvegarder les contrôleurs de domaine AD ne signifie pas automatiquement que l'outil peut vous aider à récupérer rapidement votre forêt AD si votre schéma est corrompu ou que tous vos DC ont été infectés par un logiciel malveillant ou une quelconque cyberattaque. Il faut savoir que la plupart des solutions de sauvegarde centrées sur les sauvegardes au niveau du système d'exploitation peuvent être efficaces pour la récupération de serveurs individuels, voire de contrôleurs de domaine, mais ne sont pas en mesure de coordonner le processus de récupération complexe requis pour remettre votre forêt AD en état après une cyberattaque (voir la section suivante).

Un autre aspect donne à réfléchir : il existe un risque de réintroduction des logiciels malveillants qui ont pu être conservés dans le système d'exploitation Windows de vos DC AD pendant plusieurs semaines ou plusieurs mois, sans avoir été détectés. Ces logiciels malveillants peuvent se trouver dans vos sauvegardes AD si l'outil tiers effectue la sauvegarde standard SSB (System State Backup) ou BMR de vos DC, comme c'est le cas avec l'outil WSB intégré.

AUTRES RESSOURCES

LIVRES BLANCS

Assessing the ROI of a Quick Active Directory Recovery

Report: Recovering Active Directory from Cyber Disasters

WEBINAIRE

A Cyber-First Approach to Disaster Recovery

BLOGS

Now's the Time to Rethink Active Directory Security

Time to Leave ADFS Behind for Authenticating in Hybrid Environments?

The Dos and Don'ts of Active Directory Recovery

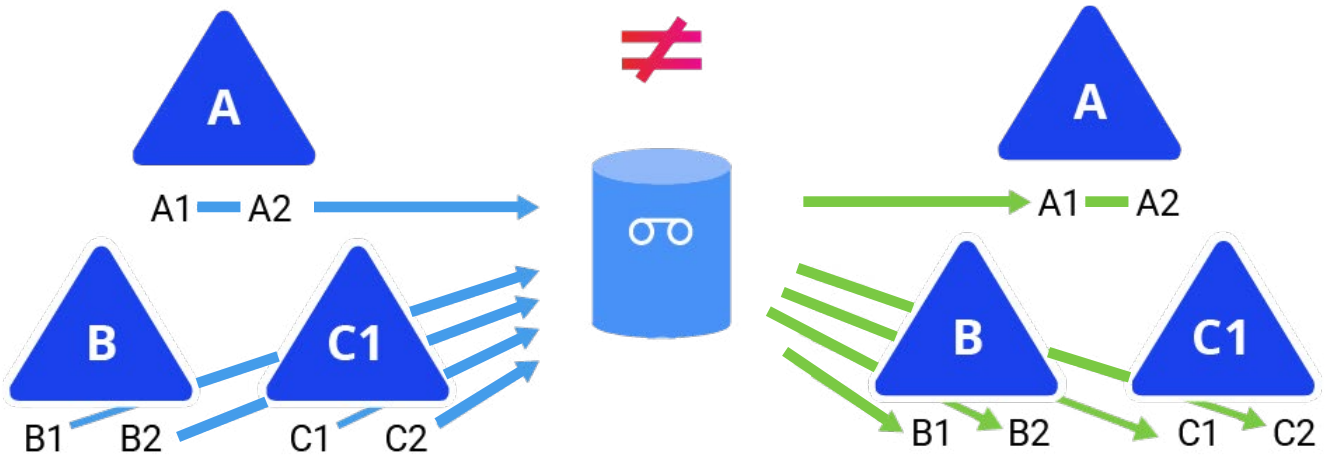
Timeline of a Hafnium Attack

RÉCUPÉRATION D'ACTIVE DIRECTORY

En matière de récupération d'Active Directory, il importe de bien distinguer la récupération des données (utilisateurs, groupes, ordinateurs, stratégie de groupe, etc.) de la récupération du service AD, c'est-à-dire de l'application distribuée exécutée sur plusieurs serveurs désignés contenant la charge de travail des services de domaine Active Directory, configurés selon une topologie spécifique. Cette tâche est d'autant moins aisée que tous les contrôleurs de domaine de la forêt partagent la configuration de la topologie AD et le schéma de la base de données au sein de leur propre base de données AD.

De bonnes sauvegardes du contrôleur de domaine

ne sont PAS synonymes d'une récupération simple des services AD



Sauvegarde de DC

Récupération de DC

Une récupération totale de la forêt doit être réalisée conformément au Guide de récupération de forêt Active Directory de Microsoft.

Ce n'est pas parce que vous avez sauvegardé tous les contrôleurs de domaine AD requis que vous pouvez facilement restaurer l'ensemble du service AD, c'est-à-dire toute la forêt AD, en cas de sinistre réel. Lorsque des logiciels malveillants détruisent tous vos DC, il vous faudra subir le douloureux processus de récupération de votre AD à partir d'une installation minimale.

Le processus de récupération de la forêt Active Directory peut être pénible

Comme évoqué précédemment, dans le panorama des menaces de plus en plus vulnérables qui pèsent sur les systèmes informatiques, ce sont les réseaux, les applications et la sécurité des identités (et non la géographie) qui déterminent l'ampleur d'un sinistre. La tolérance aux pannes obtenue grâce aux multiples centres de données devient inutile face à des logiciels malveillants sophistiqués qui se propagent en quelques minutes sur un réseau.

Le spectre d'une forêt AD entièrement détruite est ainsi passé du stade de rêve agité chez les administrateurs AD à celui de réalité.

Tout récemment, les clients de Microsoft ont été confrontés à une nouvelle attaque majeure contre un produit très étroitement intégré à leur système AD sur site : quatre nouvelles vulnérabilités de type « zero-day » dans Microsoft Exchange ont permis au groupe cybercriminel chinois « Hafnium » d'injecter un code malveillant dans les serveurs Exchange de plus de 30 000 entreprises, avant que les serveurs ne bénéficient de correctifs appropriés. Cette attaque a permis aux pirates de prendre le contrôle total et à distance des systèmes concernés. En raison de la généralisation des autorisations Microsoft Exchange dans Active Directory, ce dernier constitue une autre cible facile. AD serait probablement infiltré dans un premier temps pour accroître les privilèges des pirates et obtenir des données sensibles sur l'entreprise attaquée. Ces données seraient ensuite copiées sur une cible externe placée sous le contrôle des pirates. Dans un deuxième temps, les pirates prendraient un jour ou une semaine pour diffuser et distribuer le ransomware au plus grand nombre de systèmes auxquels ils ont accès. Pendant ce temps, l'entreprise cible ne se rend pas encore compte qu'elle a été piratée et se contente de sauvegarder les systèmes infectés dans le cadre de sa routine quotidienne de sauvegarde (selon FireEye, un pirate reste en moyenne 72 jours sans être détecté au sein d'un réseau corrompu). Éventuellement, il déclenche le ransomware qui crypte les systèmes affectés, à savoir tous les systèmes de l'entreprise membres d'AD, et tous les contrôleurs de domaine AD eux-mêmes. Enfin, les cybercriminels responsables demandent une énorme rançon à l'entreprise victime en échange de la promesse (sans garantie aucune) de fourniture d'une clé de décryptage et de non-revente des données volées.

Pourquoi ne pas simplement effectuer une récupération à partir des sauvegardes ?

Donc, dans le cas d'un véritable sinistre affectant votre service AD, pourquoi ne pas simplement restaurer tous vos DC à partir de sauvegardes ? Comme indiqué précédemment, une « bonne sauvegarde » des services pour lesquels le rôle AD DS a été installé (les contrôleurs de domaine) ne signifie pas qu'il est facile de récupérer le service Active Directory. Il y a de nombreuses étapes à suivre pour restaurer votre service AD vers un état sécurisé.

> ***Pour réussir le processus de récupération, une coordination est nécessaire entre les ingénieurs AD, les équipes chargées des opérations de récupération et, le plus souvent, les équipes de gestion de la virtualisation, à chaque emplacement où vous avez l'intention de récupérer vos DC.***

Le processus de récupération d'AD

De nombreux administrateurs AD se sont convaincus progressivement qu'ils maîtrisaient la situation. Pourtant, le moment venu, il ne suffit pas de suivre les instructions du Guide de récupération de forêt Active Directory. Et le processus n'est pas le seul à rendre difficile la récupération des forêts : cela représente également un défi sur le plan de la logistique et de la formation. Pour réussir le processus de récupération, une coordination est nécessaire entre les ingénieurs AD, les équipes chargées des opérations de récupération et, le plus souvent, les équipes de gestion de la virtualisation, à chaque emplacement où vous avez l'intention de récupérer vos DC. Chacun doit exécuter ses tâches de manière irréprochable, dans un ordre précis, et dans un contexte où le stress est probablement le plus élevé de toute sa carrière.

Feuille de route détaillée pour une reprise de forêt AD

Voici un bref aperçu des étapes à suivre pour restaurer une forêt AD vers un état de sécurité connu :

1. Déterminer la structure de la forêt et les sauvegardes disponibles

2. Identifier un DC unique par domaine, avec sauvegarde valide

3. Arrêter tous les DC de la forêt

4. Récupérer en premier lieu le domaine racine de la forêt

5. Ensuite, récupérer un DC par domaine enfant

6. Nettoyer et promouvoir à nouveau tous les autres DC de la forêt

   - Vous devez récupérer la hiérarchie de confiance et les enregistrements des ressources DNS critiques.

   - Vous devez procéder à la récupération des domaines parent avant celle de leurs domaines enfant, pour préserver la hiérarchie de confiance.

La reprise après sinistre AD ne va pas de soi

La reprise après sinistre AD n'est pas une tâche de tout repos. Idéalement, vous devez vous préparer en réalisant une analyse approfondie des risques liés à votre propre environnement : La stratégie de réduction des risques est-elle trop coûteuse, et le risque résiduel est-il trop élevé ?

Vous devez impliquer, outre l'équipe qui gère Active Directory, des équipes supplémentaires (par exemple, l'équipe de réponse aux incidents), afin de relever ce défi. Vous devez définir des critères clairs pour la mise en œuvre du plan AD DR et les responsabilités en matière d'exécution. Et les conjuguer à une stratégie de communication claire.

Par-dessus tout, vous devez réfléchir soigneusement aux investissements à réaliser pour la prévention des sinistres, qui peuvent être moins coûteux qu'une reprise après sinistre.

À propos des auteurs

GUIDO GRILLENMEIER occupe le poste de Technologue en chef chez Semperis. Basé en Allemagne, Guido a été nommé MVP Directory Services par Microsoft 12 fois. Il a passé plus de 20 ans chez HP/HPE en qualité d'Ingénieur en chef. Il intervient fréquemment dans le cadre de conférences technologiques et contribue à des revues techniques. Il est le coauteur de l'ouvrage « Microsoft Windows Security Fundamentals ». Il a aidé de nombreux clients à sécuriser leur environnement Active Directory, et les a accompagnés dans leur transition vers Windows 10/m365 et vers les services cloud Azure.

GIL KIRKPATRICK occupe le poste d'Architecte en chef produits chez Semperis. Gil élabore depuis de nombreuses années des produits commerciaux destinés à l'informatique d'entreprise, en mettant l'accent sur la gestion des identités et sur les produits liés à la sécurité. Il a été nommé 15 fois Microsoft MVP pour Active Directory et Enterprise Mobility, est l'auteur de « Active Directory Programming » et a créé la Directory Experts Conference. Gil intervient sur les thèmes de la cybersécurité, de l'identité et de la reprise après sinistre dans de nombreuses conférences informatiques à travers le monde.

+1-703-918-4884
info@semperis.com
www.semperis.com

221 River Street
9th Floor
Hoboken, NJ 07030

Pour les équipes de sécurité chargées de défendre les environnements hybrides et multicloud, Semperis garantit l'intégrité et la disponibilité des services d'annuaire d'entreprise critiques à chaque étape de la chaîne de destruction cybernétique et réduit le temps de récupération de 90 %. Conçue pour sécuriser les environnements Active Directory hybrides, la technologie brevetée de Semperis protège plus de 50 millions d'identités contre les cyberattaques, les violations de données et les erreurs opérationnelles. Les plus grandes organisations du monde font confiance à Semperis pour détecter les vulnérabilités des annuaires, intercepter les cyberattaques en cours et se remettre rapidement des attaques de ransomware et autres situations d'urgence liées à l'intégrité des données. Basée dans le New Jersey, Semperis est présente à l'international, avec une équipe de recherche et de développement répartie entre San Francisco et Tel-Aviv.

Semperis est l'organisateur de la conférence Hybrid Identity Protection (www.hipconf.com), qui a été primée. L'entreprise a reçu les plus hautes récompenses du secteur, et a été récemment placée au 157ème rang du classement Inc. 5000. Elle est également la quatrième entreprise de la Tri-State Area en termes de rapidité de croissance et la 35ème du classement général Technology Fast 500™ de Deloitte en 2020. Semperis est accréditée par Microsoft et reconnue par Gartner.

semperis