semperis

2021

Rapport sur la sécurité d'Active Directory *du premier semestre 2021*

Obtenez des informations et des ressources pour améliorer la sécurité des identités hybrides

POINT DE VUE DU CEO SUR L'AVENIR
AVEC MICKEY BRESMAN

Les fondamentaux de la sécurité des identités doivent faire l'objet d'une attention particulière pour déjouer les cyberattaques

À l'issue d'un semestre de montée en puissance des cyberattaques dans tous les domaines d'activité et partout dans le monde, le CEO Mickey Bresman revient sur les tendances qui vont définir les mesures à prendre dans l'immédiat contre les attaques visant les revenus des entreprises, la sécurité publique et nationale.

Pourquoi les entreprises ont-elles encore des difficultés à appliquer les fondamentaux de la sécurité de l'Active Directory?

Tout d'abord, Active Directory existe depuis 20 ans et à ces débuts la sécurité n'était pas nécessairement une priorité absolue pour les équipes chargées de sa configuration. Il faut ajouter à cela que l'AD est désormais bien plus compliqué : tout environnement a de nombreux niveaux d'autorisations et autres paramètres complexes.

L'AD reste le cœur battant de la gestion d'identités, le cœur de la plateforme d'identités pour la plupart des organisations, mais tout le reste a changé rapidement. L'hygiène de base de l'AD ne posait pas problème il y a 15 ans. Par conséquent, une bonne partie des erreurs faites hier sont devenues les problèmes d'aujourd'hui. Je voudrais aussi dire un mot sur le manque de compétences nécessaires, car vous avez des gens qui connaissent parfaitement l'AD, mais raisonnent plutôt en termes opérationnels. D'autres connaissent sur le bout des doigts les procédures d'urgence et la sécurité, mais ne sont pas des experts de l'AD. Il est difficile de trouver une personne réunissant cette combinaison de compétences.

Comment les entreprises peuvent-elles agir sur les compétences ou la structure organisationnelle pour décloisonner les équipes IT et de sécurité?

L'identité doit absolument faire partie de l'approche générale de la cybersécurité de l'entreprise. Toute personne responsable de l'identité doit mettre la cybersécurité au premier plan. Sachant que de nombreuses organisations dépendent de l'Active Directory pour maintenir leurs opérations après une cyberattaque, comment retrouver un fonctionnement normal aussi rapidement que possible si le pire se produit ? Certaines sociétés ont amorcé le processus de transfert de la responsabilité de l'identité à l'équipe de sécurité. Et même dans les organisations où l'identité reste gérée sous l'angle opérationnel, les informaticiens sont davantage sensibilisés à la sécurité et l'on constate une meilleure collaboration entre les équipes de sécurité et IT, notamment pour la gestion de l'identité et l'Active Directory.

C'est une tendance encourageante à mon avis : si vous êtes responsable de l'une des facettes de l'identité, vous devez donner la priorité à la sécurité.

Quels défis de sécurité découlent de la gestion d'un environnement d'identité hybride ?

La gestion des environnements d'identité hybride présente de nombreux challenges, à commencer par le fait que l'Active Directory et l'Azure Active Directory n'ont pas grand-chose en commun hormis leur nom. Azure AD utilise une pile de protocoles différents et, par conséquent, implique une approche de gestion très différente, y compris pour la protection du système d'identité contre les cyberattaques. Par exemple, si je modifie les identités dans le cloud, est-ce que cela affecte ma position de sécurité générale dans le centre de données, à savoir l'environnement sur site ? Dans un scénario hybride, la surface d'attaque potentielle est plus étendue. Il est relativement courant de voir des attaques commencer sur site, puis se propager sur le cloud, ou inversement. Les organisations doivent dès maintenant réfléchir aux modifications apportées aux systèmes d'identité dans chaque environnement, et se demander si la connectivité entre les deux risque de créer un point d'entrée pour les pirates.

La gestion de la sécurité dans un environnement hybride met également au premier plan le modèle de responsabilité partagée. La responsabilité de Microsoft est de s'assurer que le service continue de fonctionner et ce que vous faites ensuite de votre environnement, y compris sa sécurisation, relève de votre responsabilité.

Combien de temps l'environnement hybride sera-t-il en jeu pour la plupart des organisations ?

La majorité de nos clients n'abandonneront jamais la totalité de leur centre de données. Le modèle hybride pourrait bien rester en place indéfiniment. Les entreprises feront le tri entre ce qu'il est préférable de gérer depuis le centre de données et ce qu'il vaut mieux utiliser en tant que service (aaS) confié à Microsoft, AWS, Google ou tout autre prestataire. Elles ont désormais un vrai choix de solutions en fonction de leur situation et des besoins. Le cloud n'est pas une solution universelle.

Mais quelle que soit la proportion de systèmes et de ressources sur site et cloud, il n'en reste pas moins vrai que le référentiel d'identité doit être protégé. L'identité restera un élément majeur du jeu de protection que nous menons face à nos adversaires. Il est également acquis que l'importance de la protection de l'identité ne cessera de croître au fur et à mesure de la progression de vos processus de numérisation et d'adoption du cloud.

LÂCHER PURPLE KNIGHT

Purple Knight donne aux équipes IT et sécurité les moyens d'identifier les lacunes d'Active Directory

Cet outil de sécurité, téléchargé des milliers de fois, évalue gratuitement le degré de sécurité de l'AD, afin d'identifier et de combler les lacunes généralement visées par les cyberattaques

La publication de l'outil d'évaluation Purple Knight en mars 2021 répond au besoin non satisfait d'identification et de comblement des lacunes de sécurité de l'Active Directory. Des milliers d'informaticiens et de professionnels de la sécurité ont téléchargé cet outil gratuit, développé par les experts de l'identité de Semperis, qui recherche dans l'environnement de l'Active Directory plus de 60 indicateurs d'exposition (IOE) et de compromission (IOC).

« Aucun d'entre nous n'imaginait un tel taux d'acceptation de Purple Knight sur le marché », explique Mickey Bresman, CEO de Semperis. « Mais c'est une bonne surprise, car les organisations font désormais un lien direct entre les attaques dont ils entendent parler et les points faibles de l'Active Directory. Purple Knight leur permet de faire le point sur l'état de préparation de leur environnement AD par rapport à ces différents types d'attaque. »

Toujours selon Mickey Bresman, les retours des clients laissent entendre que Purple Knight identifie des vulnérabilités que même les cabinets de conseil manquent, un avantage qu'il attribue non seulement à l'expertise de l'équipe de Semperis, mais aussi à la façon dont les organisations utilisent l'Active Directory.

« Nous avons constaté que de nombreuses entreprises ne connaissent pas précisément les failles de l'Active Directory », explique Mickey Bresman. « Nous voulions donner aux équipes de sécurité qui ne maîtrisaient pas l'AD une solution pour comprendre leur position de sécurité, puis combler les lacunes pour réduire leur surface d'attaque. »

Purple Knight analyse l'environnement AD pour identifier les lacunes de sécurité résultant d'une activité malveillante ou des erreurs de configuration qui sont passées inaperçues pendant des années. Ran Harel, responsable senior des produits de sécurité chez Semperis, ajoute que la plupart des erreurs de configuration qu'il constate dans les déploiements de l'Active Directory résultent d'une mauvaise compréhension du modèle global de sécurité ou de correctifs rapides qui génèrent des failles de sécurité par la suite.

« Ces scénarios sont une cible privilégiée en cas d'attaque, notamment les configurations erronées avec Kerberos et les stratégies de groupe », résume Ran Harel.

Voici quelques-unes des vulnérabilités les plus fréquemment découvertes par Purple Knight :

- Mots de passe qui n'ont pas été modifiés fréquemment, laissant l'entreprise exposée aux attaques par force brute
- Comptes dont les privilèges ont été élevés sans vérification adéquate, par exemple, le groupe Administrateurs de clés d'entreprise
- Comptes Exchange pour lesquels des autorisations AD ont été élevées et qui ont proliféré au fil du temps
- Délégations Kerberos configurées « sans limitation », un scénario facile à détourner ou qui risque de vous exposer accidentellement à des utilisateurs malveillants
- Configuration faible des stratégies de groupe créant des vulnérabilités de sécurité lorsqu'elles sont liées à l'Active Directory au niveau du domaine.

“Nous voulions donner aux équipes de sécurité qui n’ont pas une expertise approfondie de l’AD un moyen de comprendre leur posture de sécurité AD, puis de combler les lacunes existantes afin que les attaquants ne les utilisent pas contre eux. ”

Mickey Bresman, *Semperis* CEO

Purple Knight génère un score de risque global de l’AD, ainsi qu’une série de scores individuels dans les catégories de la délégation AD, de la sécurité des comptes, de l’infrastructure AD, ainsi que la sécurité des stratégies de groupes et la sécurité Kerberos. Dans les rapports Purple Knight initiaux, le score moyen des organisations était de 61 %, soit à peine la moyenne. La sécurité Kerberos était la catégorie au score le plus faible :

Scores moyens des évaluations initiales

SCORE GLOBAL	61%
Délégation AD	**68%**
Sécurité des comptes	**59%**
Sécurité de l’infrastructure AD	**77%**
Sécurité des stratégies de groupe	**58%**
Sécurité Kerberos	**43%**

Les cybercriminels voient les autorisations de domaine laxistes comme des fruits mûrs prêts à cueillir, explique Darren Mar-Elia, vice-président produits chez Semperis.

« Ces failles sont très prisées par les attaquants, parce qu’elles leur facilitent la tâche », confie Darren Mar-Elia. « Les attaquants recherchent toujours le chemin le plus court pour accéder au compte d’administrateur de domaine, car une fois qu’ils l’ont trouvé, tout est joué. »

Une protection constante contre des failles de sécurité de l’AD nécessite une bonne hygiène de compte, martèle Ran Harel, responsable produits principal de Semperis.

« Mais c’est notoirement difficile à faire », explique Ran Harel. « Un utilisateur peut appartenir à 20 groupes différents, qui peuvent eux-mêmes comporter des sous-groupes ayant des droits délégués. Les autorisations sont comme des spaghettis, il faut les lancer contre un mur pour savoir si elles bonnes. Si vous ne le faites pas, la gestion de compte se délite et les problèmes s’aggravent. »

Paradoxalement, les rapports de Purple Knight relèvent que les plus grandes organisations, pourtant mieux dotées en ressources, sont aussi les plus susceptibles d’avoir pris du retard sur la sécurisation de leurs systèmes d’identité critiques en raison de la taille et de la complexité de leur environnement, ce qui les expose à une attaque de type Solar Winds.

“Etant donné qu’Active Directory est une cible de choix pour les attaquants qui tentent de voler des informations d’identifications et de déployer des ransomwares, il vaut la peine de considérer les répercussions d’une attaque Active Directory même si vous n’êtes pas directement responsable de exploitation au quotidien. ”

MICKEY BRESMAN
Semperis CEO

ACTIVE DIRECTORY EST LE TALON D'ACHILLE DE LA SECURITE DES ENTREPRISES

Le PDG de Semperis appelle les leaders de la sécurité à défendre Active Directory

Active Directory est trop souvent considéré comme un simple service à récupérer parmi d'autres en cas d'attaque. Mais la réalité est qu'AD est une véritable clé de voûte : si elle est compromise, tout votre environnement le sera aussi.

Près de la moitié (47 %) des organisations utilisent Active Directory comme magasin d'identités principal. 51 % l'utilisent avec d'autres magasins d'identités et lui accordent une importance variable par rapport à ces derniers. Toutefois, seulement 1 % des organisations n'utilisent pas du tout AD ou procèdent à son retrait.

De nombreuses organisations adoptent une approche hybride de la sécurité et commencent à s'intéresser aux interdépendances cloud et aux complexités qui en résultent, mais ignorent le fait que l'intégralité de leur identité cloud reste synchronisée avec la version sur site d'Active Directory. AD est utilisé en tant que source de synchronisation des autres magasins d'identités, par conséquent, toute violation d'AD peut avoir un effet boule de neige, car AD crée des liens avec les autres applications cloud. Cette connexion potentiellement problématique entre les ressources cloud et sur site risque de s'aggraver alors que les organisations se réorganisent aussi rapidement que possible pour assister les salariés qui doivent utiliser des appareils mobiles pendant la pandémie.

Dans « Repenser la sécurité d'Active Directory» sur Help Net Security, le PDG de Semperis Mickey Bresman explique à quel point il est important d'avoir un plan d'action éprouvé pour la récupération d'Active Directory (AD) en cas de cyberattaque. Vous trouverez plus de détails dans cet article sur les mesures que les entreprises peuvent prendre pour se protéger contre les cyberattaques en relation avec AD, notamment pour mettre en place des mesures propres à AD.

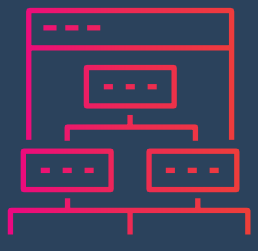
MORE RESOURCES

BLOGS

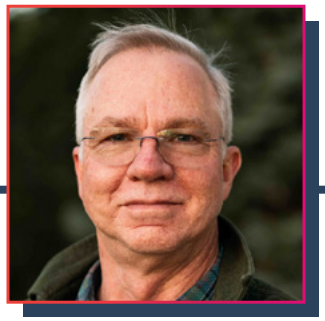
- Semperis Expert: SolarWinds Attack Highlights Need to Secure AD
- CISA's Ransomware Guidance Is Reminder to Include AD in Recovery Plan

WEBINAR

- What You Need to Know About Securing Active Directory



CONSTRUIRE UNE ORGANISATION CYBER-RESILIENTE



Les experts de l'Active Directory ont un avenir dans la sécurité

PAR **GIL KIRKPATRICK,** *Chief Architect chez Semperis*

La croissance des applications cloud et un contexte de menace en pleine évolution ont profondément transformé l'univers des professionnels des systèmes Microsoft Active Directory (AD).

Comme pour les autres domaines de l'informatique, la motivation et la curiosité, indispensables pour élargir ses compétences, comptent parmi les attributs essentiels pour les ingénieurs et les architectes spécialisés dans l'AD.

Après avoir consacré deux décennies aux systèmes sur site ainsi qu'aux utilisateurs et aux applications, la plupart des ces professionnels de l'AD sont désormais chargés de l'intégration cloud et de la sécurité de l'accès à des environnements pour lesquels le périmètre réseau traditionnel a disparu. D'autre part, ils doivent opérer cette transition, alors que les attaquants utilisent des outils de plus en plus élaborés, qui exploitent les erreurs de configuration de l'AD et les failles de Windows, ciblent les identifiants de connexion des utilisateurs, et tentent d'établir une menace persistante sur site.

Face à cette situation, les responsables techniques savent qu'il faut faciliter la coopération entre les équipes de sécurité et d'identité pour garantir un accès sécurisé à l'époque du cloud computing et du télétravail généralisé.

Pour ce qui est de l'avenir, les experts de l'AD doivent s'attendre à jouer un rôle plus actif dans les discussions de sécurité. Cet usage n'est pas encore très répandu, mais alors que l'AD reste une surface d'attaque de choix pour les cybercriminels, les spécialistes peuvent saisir cet instant pour mettre à profit leur expertise en contribuant à l'effort collectif de renforcement de la sécurité de l'entreprise. Alors que l'identité est au centre des stratégies de sécurité et que les administrateurs de l'AD sont de plus en plus sollicités lors des conversations sur la sécurité, ceux qui parviennent à élargir leur socle de connaissances et de compétences apporteront davantage de valeur à l'entreprise.

L'évolution du contexte de sécurité crée également des opportunités pour les professionnels de l'Active Directory

À bien des égards, l'AD n'a pas été conçu pour répondre aux challenges actuels de sécurité, mais ses vulnérabilités, telles que la faille exploitée par les attaques Zerologon l'an dernier, ne sont pas seules en cause. Les attaquants modernes exploitent également les protocoles incorporés dans le système d'exploitation Windows, et notamment l'AD lui-même.

De plus, il y a le problème des ransomwares. Des attaques APT (Advanced Persistent Threat) de reconnaissance et de vol d'informations utilisant comme vecteur des outils tels que BloodHound et Mimikatz ont été observées ces dernières années. En 2020, un ransomware a utilisé le partage SYSVOL de contrôleurs de domaines AD pour implanter du code malveillant dans l'environnement cible.

Dans le passé, la planification de récupération de l'AD visait essentiellement des événements tels que des catastrophes naturelles, des pannes de courant ou des erreurs d'administration. Mais à présent, la probabilité d'un ransomware perturbant l'intégralité des opérations informatiques est bien plus élevée et le risque de reconstitution de l'intégralité de l'AD doit faire l'objet de préparations spécifiques.

Placer l'identité avant tout

Les utilisateurs mobiles et le Cloud Computing ont érodé le périmètre réseau traditionnel : le seul point de contrôle pour les utilisateurs, les applications et les ressources réseau est l'identité de l'utilisateur. L'identité numérique touche tous les aspects de l'entreprise moderne. Chaque utilisateur doit pouvoir accéder aux systèmes et aux applications métier. Cela ne veut pas dire pour autant que le contrôle d'accès sécurisé est une simple question de productivité. Un nombre excessif d'autorisations, des mots de passe faibles et de nombreux autres problèmes latents est sont source de failles de données, d'infections par du code malveillant, de pertes financières considérables, sans parler des longues nuits gâchées pour les responsables informatiques et l'équipe de direction.

Le développement constant de l'écosystème d'applications cloud utilisé par les salariés crée des challenges d'intégration avec l'AD qui ne concernent pas seulement l'équipe de sécurité. L'extension sur le cloud des stratégies d'accès et de sécurité conçues pour l'AD sur site est également un problème de sécurité. Les experts de l'AD habitués au modèle d'autorisation de leur environnement sur site risquent de trouver difficile le changement de mentalité nécessaire pour intégrer l'AD sur site avec Azure Active Directory (AAD). (Pour une discussion plus détaillée des implications de la gestion simultanée de l'AD sur site et de l'AAD dans un environnement hybride, lisez « Principaux risques de sécurité à surveiller lors de la transition vers la gestion d'identité hybride » par Doug Davis, responsable produit senior chez Semperis.)

Mais comme toujours, le changement est aussi source d'opportunité. Connaître les nouveaux risques auxquels une organisation est confrontée, et la place de l'AD dans le puzzle de sécurité, est un atout majeur lors des efforts de transformation numérique. Les spécialistes de l'identité dont l'expertise est reconnue lors des échanges avec l'équipe de sécurité ou de direction seront mieux placés pour contribuer au plan de sécurité de l'entreprise et élargir leur horizon professionnel.

Actualisation des connaissances en identités et sécurité

Pour les professionnels de l'Active Directory et autres services d'identité qui souhaitent contribuer à la stratégie de sécurité de l'entreprise, la clé est de tenir ses connaissances à jour, ce qui est à la fois l'un des aspects les plus difficiles et les plus motivants d'une carrière dans l'informatique. Pensez à toutes les technologies que les informaticiens ont utilisées au cours de leur carrière et qui sont maintenant dépassées. Combien de technologies ont atteint la fin de leur cycle de vie et ne sont plus prises en charge ? L'apprentissage constant est essentiel pour s'adapter aux réalités mouvantes de la sécurité informatique et des opérations.

La bonne nouvelle est que vous trouverez des ressources abondantes pour les informaticiens sur Internet. Channel 9, par exemple, est une excellente ressource de vidéos pédagogiques sur les produits Microsoft. Microsoft fournit également des guides de préparation pour ses examens de certification. Les professionnels de l'identité ont tout à gagner en préparant des certifications de sécurité MS telles que « Security, Compliance, and Identity Fundamentals » et « Security Fundamentals ». Ces certifications, entre autres, ne servent pas seulement à consolider un CV, mais permettent d'acquérir des bases solides en concepts de sécurité qui seront très utiles lors des échanges avec les responsables techniques.

Mais rien ne vaut l'expérience. Une expérience pratique en laboratoire, non seulement avec la version sur site d'AD, mais aussi dans les environnements hybrides utilisant Azure, AWS et Google Cloud Platform, est le seul moyen d'obtenir les compétences nécessaires pour une gestion efficace et sécurisée.

Restez un éternel étudiant en identité et sécurité

L'évolution de carrière en informatique n'a qu'une seule constante, le changement. Aspirer à la maîtrise de tous les aspects de l'industrie, de la sécurité au développement d'applications, implique la volonté de rester au fait des différentes technologies et tendances. Dans un contexte d'augmentation des risques de sécurité liés à l'identité et de montée en puissance du cloud, les professionnels de l'AD doivent non seulement comprendre, mais mener les débats sur la place de la gestion d'identité dans la stratégie de sécurité de leur entreprise.

Renforcement de l'Active Directory en trois étapes pour tirer les leçons des attaques récentes

PAR **BRIAN DESMOND,** *Principal chez Ravenswood Technology Group*

Au cours d'un séminaire récent que j'ai co-animé avec Semperis (la société derrière l'outil d'évaluation de la sécurité Purple Knight), nous avons parlé principalement du dénominateur commun des attaques majeures récentes : l'Active Directory. Au cours de la session « How Attackers Exploit Active Directory: Lessons Learned from High-Profile Breaches » (Comment les attaquants exploitent Active Directory : leçons à tirer des violations majeures), Sean Deuby et Ran Harel de Semperis se sont joints à moi pour parler de quatre attaques récentes très médiatisées, à savoir SolarWinds, les attaques 0-day Hafnium sur Exchange, Colonial Pipeline et Ireland Health Service. Si ces violations sont très différentes en termes de tactique et d'origine des pirates, elles ont toutes eu des conséquences dévastatrices. Au cours de notre discussion, nous avons couvert trois des mesures préventives les plus importantes à prendre pour protéger une entreprise contre les cyberattaques.

1 Protéger les e-mails contre les menaces avancées

La messagerie est le point d'entrée le plus fréquent lors des attaques. Les campagnes d'hameçonnage avancées sont extrêmement convaincantes pour les utilisateurs et ouvrent de véritables boulevards pour s'approprier des identifiants de connexion valides et/ou implanter du code malveillant sur les terminaux. Il est par conséquent essentiel que les organisations adoptent une approche multidimensionnelle pour se protéger contre ces menaces. La sensibilisation à la sécurité et les simulations d'hameçonnage sont importantes pour comprendre et mesurer les risques. Mais quel que soit le nombre de formations que vous mettrez en place, les attaquants finiront par arriver à leurs fins. Pour contrer cela, une solution de protection avancée des e-mails, allant au-delà des simples outils antispam et antivirus, doit être intégrée dans votre stratégie de protection. Un service utilisant des algorithmes d'apprentissage machine et autres mesures de détection avancées pour détecter et bloquer les messages d'hameçonnage, ainsi que les pièces jointes suspectes, doivent être mis en place dans le contexte actuel de menaces.

« À moins d'avoir vécu au fond d'une caverne pendant toute l'année écoulée, il est difficile d'ignorer les événements significatifs de cybersécurité qui se sont déroulés semaine après semaine. Nous avons passé beaucoup de temps à parler des nouveaux angles d'attaque, mais en réalité, les acteurs de ces menaces ne recherchent pas la nouveauté, ils veulent juste trouver une voie d'accès et voient Active Directory comme une autoroute . »

— SEAN DEUBY, *Directeur des Services chez Semperis*

2 Prévenir les déplacements latéraux

Dès qu'un ordinateur client ou un serveur membre est compromis, les attaquants tentent de se déplacer latéralement sur le réseau et d'élever leurs privilèges. Le blocage du mouvement latéral complique singulièrement la tâche des attaquants. Vous pouvez mettre en place des mesures techniques simples, même si elles paraissent parfois compliquées d'un point de vue opérationnel, pour bloquer les déplacements latéraux. Tout d'abord, le mot de passe administrateur local de chaque terminal doit être différent. Microsoft propose une solution gratuite appelée LAPS (Local Administrator Password Solution) pour ce faire. Deuxièmement, vous ne pouvez pas incorporer des comptes de domaine dans le groupe des administrateurs locaux pour simplifier le support informatique. Les informaticiens doivent utiliser LAPS pour récupérer les identifiants d'administration de terminaux spécifiques.

3 Sécuriser l'accès aux identifiants de connexion privilégiés

Empêcher les cybercriminels d'obtenir un accès privilégié, surtout en tant qu'administrateur de domaine, est une défense essentielle. En effet, si un pirate parvient à élever ses privilèges, il risque de contrôler une plus grande partie du réseau, voire son intégralité. L'implémentation de mesures efficaces qui isolent et protègent les identifiants avec privilèges est donc très importante. Deux des contre-mesures les plus communes que Ravenswood Technology Group implémente sont les concepts de mesures de sécurité hiérarchisées et de stations de travail à accès privilégié (PAW). Les mesures de sécurité hiérarchisées empêchent les identifiants à privilèges élevés d'être accessibles par des ressources à plus haut risque, comme des ordinateurs clients où les identifiants peuvent être volés. Les PAW isolent les tâches que l'administrateur réalise depuis sa station de travail ordinaire sur une station hautement sécurisée, protégeant ainsi les identifiants et la session de l'administrateur contre des vecteurs de menaces tels que la messagerie, l'accès Internet et certains types de code malveillant.

MORE RESOURCES

VIDEO

↗ **Active Directory security pro tip:** Staying ahead of ransomware attacks that exploit AD

BLOG

↗ How to Defend Against Ransomware-as-a-Service Groups That Attack Active Directory

DOWNLOAD PURPLE KNIGHT

↗ Identify and address AD security gaps and gain confidence in the security of your AD environment

Votre AD est-il prêt dans le contexte actuel des menaces ?

Les attaques dont nous avons parlé au cours du webinaire ne représentent que quatre des innombrables violations qui font la une quotidiennement. Il est vital de renforcer l'environnement informatique de votre organisation et pour quasiment toutes les entreprises, l'Active Directory doit devenir un composant essentiel de la stratégie de renforcement. N'hésitez pas à essayer la version gratuite de Purple Knight pour évaluer les contrôles de sécurité de l'Active Directory. En dehors de Ravenswood et Semperis, il n'existe probablement pas deux autres organisations (en dehors de Microsoft naturellement) combinant davantage d'expertise de sécurité sur l'AD. Nous avons formé un partenariat extrêmement puissant qui permet aux organisations du monde entier de rehausser leurs mesures de sécurité basées sur l'identité hybride

Si vous recherchez des conseils pour la protection de votre organisation, consultez le webinaire à la demande. Et naturellement, vous pouvez télécharger Purple Knight gratuitement pour identifier et traiter les lacunes de sécurité de l'AD et vous redonner confiance concernant le niveau de sécurité de votre environnement AD, quel que soit son degré de complexité, de ramification ou de déshérence.

Retour sur investissement réel en cas de récupération rapide de l'Active Directory

BY **SEAN DEUBY,** *Directeur des Services chez Semperis*

Si tous les responsables IT ou administrateurs savent qu'un plan de récupération sérieux de l'Active Directory est un composant essentiel de toute stratégie de continuité métier, le calcul de son retour sur investissement réel est notoirement difficile. Trop de variables sont en jeu pour générer un calcul rigoureux et démontrable. Et afin de ne pas créer de faux espoirs, je préfère dire dès maintenant que je ne vais pas proposer de simulateur interactif de retour sur investissement ici.

Par contre, je vais examiner quelques pistes permettant de voir le retour sur investissement correspondant à une restauration correcte de l'AD, ce qui vous permettra de faire vos calculs et d'arriver à vos propres conclusions. La perte d'un contrôleur de domaine est un problème en soi, mais penchons-nous sur un autre scénario de plus en plus courant et qui peut avoir des conséquences catastrophiques : une attaque de ransomware qui désactive tous les contrôleurs de domaine sur tous les sites de l'entreprise. Dans ce cas, la récupération de l'AD est un défi qui met les nerfs à rude épreuve et qu'il faut généralement relever avec un pistolet sur la tempe.

Au cours de l'année dernière, nous avons parlé de dizaines d'attaques par ransomware où les cybercriminels ont modifié l'AD d'une façon ou d'une autre, bien au-delà des changements basiques des comptes ou mots de passe utilisateur, pour accéder aux systèmes d'information et se déplacer latéralement pour propager le code malveillant. Les architectes de ransomware peuvent désormais compter sur des ingénieurs qui passent au crible l'AD et ses mises à jour de sécurité à la recherche d'opportunités d'élévation des autorisations et de distribution rapide du code malveillant dans toute l'organisation. L'analyse scientifique des attaques précédentes de ransomware impliquant l'AD révèle que les pirates ciblent principalement la modification des comptes de groupe, des comptes d'utilisateurs, des objets de stratégie de groupe, le SYSVOL et les contrôleurs de domaine.

Connaissant ces tactiques de cybercriminalité, tenez compte des facteurs suivants lors du calcul de votre propre retour sur investissement en cas de récupération de l'AD :

Coût des pertes opérationnelles

Coût des pertes opérationnelles : il est probable qu'une partie substantielle de votre activité dépende du bon fonctionnement de l'AD pour authentifier les utilisateurs avant de leur donner accès aux applications, systèmes et données. Pour chaque heure d'indisponibilité de l'AD, quelles seraient les pertes de revenu ou de productivité de votre entreprise ? Combien d'heures, de jours, voire de semaines, votre entreprise pourrait-elle tenir avant de franchir le point de non-retour et ne plus pouvoir rétablir ses finances ? Vous souvenez-vous de l'attaque de ransomware sur la ville de Baltimore ? La phase de récupération a pris des mois et coûté plus de 18 millions de dollars.ransomware attack on the City of Baltimore? Their recovery of operations took months and cost over $18 million.

Absence de plan de continuité métier couvrant l'AD

Si votre organisation est mature, vous devez avoir un plan de continuité métier/reprise après incident précisant ce qui doit être fait pour rétablir un fonctionnement normal en cas d'interruption. La plupart des plans portent sur la perte d'infrastructure ou la perte d'un site après un désastre naturel. Mais rares sont les entreprises qui disposent d'un plan spécifique en cas de cyberattaque, notamment une attaque aussi imprévisible qu'une attaque par ransomware. Le mode de récupération de l'AD dans un scénario tel que celui-ci dépend du degré de gravité des modifications de l'AD. Vous pouvez planifier le rétablissement d'une version précédente de l'AD, mais comment ferez-vous pour identifier la dernière version véritablement sûre ? Quels systèmes, services et applications dépendant de l'AD seront affectés ou ne fonctionneront plus du tout en raison du rétablissement brutal d'un état précédent d'AD ? Êtes-vous même sûr de pouvoir trouver une sauvegarde récente, sans code malveillant, à restaurer ? En l'absence de plan ou en cas d'incapacité à comprendre ce qui a changé dans l'AD avant la récupération, votre organisation passera des heures sans fin à remédier aux problèmes liés à la récupération.

La récupération n'est pas forcément la bonne réponse

Si les altérations imputables aux pirates se limitent finalement à l'ajout d'un compte dans le groupe d'administrateur de domaines, par exemple, la récupération d'une version de l'AD datant de plusieurs jours ou du mois précédent n'est probablement pas souhaitable. Il serait sans doute plus économique de surveiller les modifications apportées à l'AD et de se ménager une possibilité de refuser la modification des comptes « protégés » (tels que le groupe Administrateur de domaine) ou de rétablir automatiquement toute modification apportée à une configuration validée.

Les considérations ci-dessus peuvent être réparties dans trois catégories de risque : le risque de récupération lente, le risque de récupération générant encore plus de travail de remédiation et enfin, le risque d'overkill, à savoir une récupération excessive par rapport à la nature des modifications apportées à l'AD.

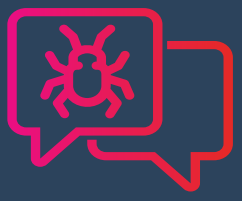
Une autre approche du calcul du retour sur investissement de la récupération de l'AD

Mieux vaut éviter les simulateurs de retour sur investissement en cas de récupération de l'AD que vous trouverez en ligne et préparer à la place différents scénarios réalistes permettant d'évaluer l'efficacité des processus en place en répondant aux questions suivantes qui s'appuient sur les facteurs esquissés ci-dessus :

- Quels éléments opérationnels critiques dépendent du bon fonctionnement de l'AD ? À combien estimeriez-vous le coût de leur interruption ?
- Combien de temps faudrait-il pour récupérer l'AD en fonction des modifications imputables à l'attaque ?
- Êtes-vous en mesure de voir les modifications malveillantes apportées à l'AD et, si ce n'est pas le cas, jusqu'où ferez-vous remonter vos investigations et combien de temps cela prendra-t-il ?
- La récupération aura-t-elle un impact sur les autres aspects de l'activité de l'entreprise que vous devrez corriger et, le cas échéant, combien de temps cela prendra-t-il ? (N'oubliez pas qu'un certain nombre d'utilisateurs et de mots de passe de comptes d'ordinateur ne vont plus correspondre, ce qui perturbera la connexion au domaine. D'autre part, les versions précédentes peuvent ne pas comporter certains comptes, membres de groupes, enregistrements DNS, etc.)
- Êtes-vous sûr que la récupération rétablira un état sécurisé connu ? Veillez à faire une distinction entre le rétablissement de l'activité métier et la récupération des activités métier : si vous ne disposez pas de sauvegardes propres et sans code malveillant comme base de récupération, vous risquez de réintroduire les failles à l'origine de l'attaque.

En résumé, le calcul du retour sur investissement de la récupération de l'AD dépend essentiellement de votre capacité actuelle à rétablir un état de production sécurisé connu, car les simulateurs en ligne ne tiennent pas compte des myriades de variables propres à une attaque par ransomware. En examinant quelques scénarios et en tenant compte de vos capacités de récupération réelles, vous identifierez des coûts qui peuvent être éliminés en mettant en place une solution adaptée de récupération de l'AD couvrant la protection contre les modifications malveillantes de l'AD, la prévention et la récupération..

QUELQUES TÉMOIGNAGES :



Semperis propose une solution « cyber-first » très prisée de reprise sur sinistre pour l'Active Directory en cas de cyberattaque. Voici quelques témoignages de nos clients ayant déployé la solution Semperis Active Directory Forest Recovery (ADFR) :

- En Israël, la compagnie El Al a déployé Semperis ADFR et ramené la durée totale de récupération de la forêt AD de 24 à 2 heures.
- Un distributeur international comptant 2,2 millions d'utilisateurs et 500 contrôleurs de domaine a remplacé la solution qu'elle avait en place par Semperis ADFR et fait passer le temps de restauration de sa forêt AD de 6 jours à 6 heures.
- Une entreprise du secteur de la santé utilisant un fichier DIT de 65 Go a réduit le temps de récupération de la forêt AD de 1,5 jour avec la solution existante à moins de 4 heures avec Semperis ADFR.

Comment se protéger contre les attaques visant l'Active Directory qui ne laissent pas de traces

PAR **GUIDO GRILLENMEIER,** *Chief Technologist chez Semperis*

Les cybercriminels exploitent de nouvelles tactiques et techniques pour accéder différemment à l'Active Directory, ce qui rend leurs attaques encore plus dangereuses et d'autant plus importantes à détecter.

La détection est l'un des éléments les plus importants de toute stratégie de cybersécurité. Avoir la capacité de repérer les méchants en train d'entrer, de se déplacer ou, encore pire, d'administrer votre réseau est essentiel pour une réponse rapide. Sachant qu'un attaquant peut rester sur votre réseau sans être détecté pendant 146 jours en moyenne, selon Microsoft, il est évident que les méchants sont passés maîtres dans l'art de la dissimulation.

Lorsqu'il faut détecter des actions potentiellement malveillantes dans l'Active Directory (AD), la plupart des organisations s'appuient sur la consolidation des journaux d'événements du contrôleur de domaine et des solutions SIEM pour identifier les connexions et les modifications anormales. Tout cela fonctionne si la technique d'attaque laisse une trace dans les fichiers journaux.

Plusieurs types d'attaque ont été constatés ici et là qui ne laissent aucune trace perceptible ou tout au moins, aucun indice d'activité malveillante. Citons quelques exemples :

Attaque DCShadow

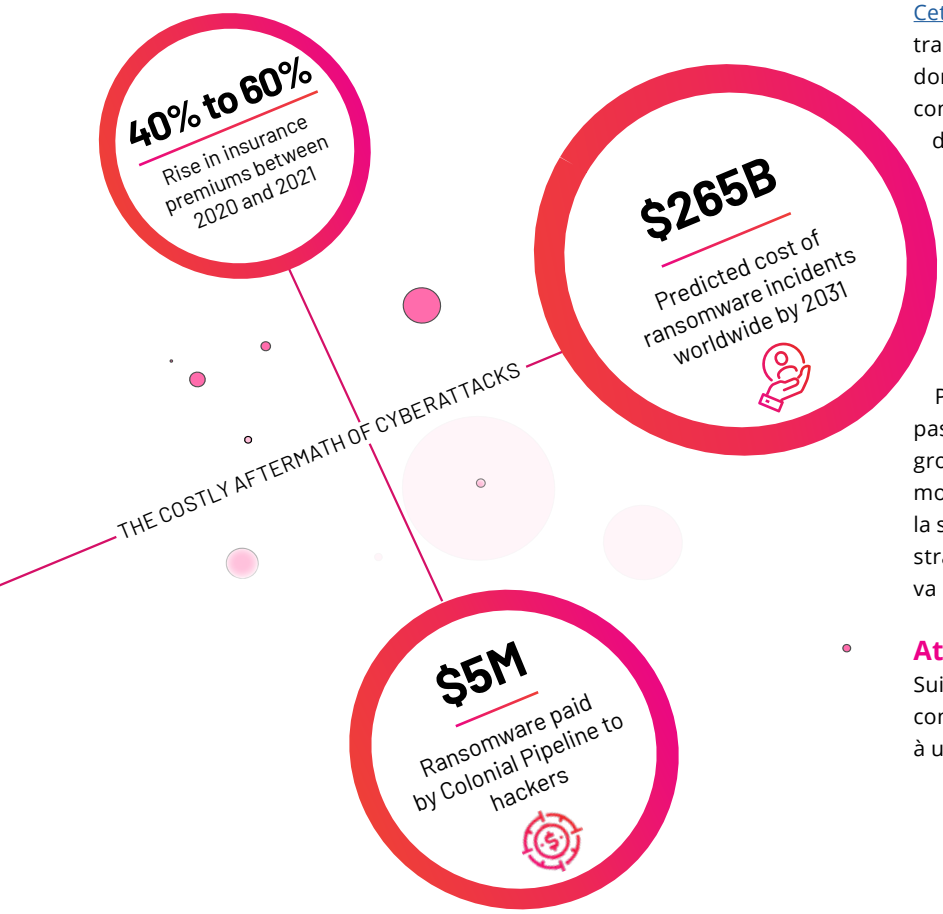
basée sur la fonctionnalité DCShadow de l'outil de piratage Mimikatz, cette attaque commence par enregistrer un contrôleur de domaine hostile en modifiant la partition de configuration de l'AD. Ensuite, le cybercriminel introduit des changements pour arriver à ses fins (p. ex., modification d'inscription aux groupes des administrateurs de domaine ou des modifications encore plus subtiles, telles que l'ajout du SID du groupe d'administrateurs de domaine à l'attribut sidHistory d'un utilisateur ordinaire qui a été compromis). Cette technique d'attaque contourne les connexions traditionnelles basées sur SIEM, car le contrôleur de domaine hostile ne signale pas les modifications. Bien au contraire, ses modifications sont injectées directement dans le flux de réplication des contrôleurs du domaine de production.

Modifications de la stratégie de groupe

Une attaque documentée impliquant le ransomware Ryuk a entraîné la modification d'un objet Stratégies de groupe qui a propagé l'installation de Ryuk sur des terminaux distants dans l'organisation ciblée. Par défaut, les journaux d'événements ne consignent pas les modifications apportées à une stratégie de groupe. Par conséquent, si un attaquant introduit des modifications (comme dans l'exemple portant sur Ryuk), la seule chose visible est qu'un compte ayant accès à la stratégie de groupe a réalisé une modification, ce qui ne va probablement pas déclencher d'alarmes.

Attaque Zerologon

Suite à la publication du code d'un exploit preuve de concept, un attaquant disposant d'un accès réseau à un contrôleur de domaine est parvenu à envoyer



des messages Netlogon spéciaux, consistant en des chaînes de zéros, ce qui a remplacé le mot de passe de l'ordinateur du contrôleur de domaine par une chaîne vide. Ainsi, sans connexion ou avec une connexion à valeur nulle, l'attaquant prend possession du contrôleur de domaine, peut réaliser des modifications dans l'AD et dispose donc d'une plateforme pour attaquer les autres systèmes de votre infrastructure. Il est peu probable que vos outils de monitoring actuels couvrent les changements de mots de passe inattendus sur vos contrôleurs de domaine.

Ce n'est pas un hasard si ces attaques ne laissent aucune trace. Les criminels ne comptent pas leurs heures et passent au peigne fin le mode de fonctionnement des environnements cibles à la recherche de solutions de court-circuitage, de brouillage et de contournement de toute forme de détection, ce qui inclut les procédures de connexion.

Ce type d'attaque étant avéré, la seule véritable question est de savoir ce qui doit être fait en matière de prévention et de réaction ?

Protection contre les modifications malveillantes de l'Active Directory

Vous pouvez protéger votre organisation contre les modifications de l'Active Directory de trois façons :

- **Monitoring des modifications de l'AD :** Cette procédure va au-delà des SIEM et nécessite une solution tierce conçue pour voir toutes les modifications apportées dans l'AD, peu importe qui en est à l'origine, du contrôleur de domaine, de la solution utilisée, etc., idéalement en lisant et interprétant le trafic de réplication des contrôleurs de domaine. Ce monitoring doit inclure également les modifications apportées à la stratégie de groupe. Dans de nombreux cas, les solutions de monitoring des modifications apportées à l'AD permettent de définir des objets protégés spécifiques dont les changements doivent être surveillés, comme par exemple, les changements d'appartenance à un groupe d'administrateurs de domaine, pour déclencher des alarmes en cas d'altération de ces objets. Cette solution doit couvrir à la fois les modifications des stratégies de groupe et la visibilité des réplications.

- **Rechercher DCShadow :** Mimikatz laissse subsister quelques artefacts et certains signes indiquent si DCShadow a bien été utilisé sur votre réseau. La recherche de ces signes dans l'AD doit faire partie d'une réévaluation régulière de sa sécurité. Notez que si vous trouvez une trace de Mimikatz DCShadow dans votre environnement, vous devrez agir rapidement, car cela signifie qu'une attaque est déjà en cours. À ce stade, vous allez vous dire qu'il aurait été bien d'avoir une solution qui montre les modifications réalisées au niveau de la réplication pour analyse et remédiation.

- **Être en mesure de récupérer l'AD :** votre organisation doit anticiper la récupération, totale ou partielle, de l'AD si vous pensez qu'il a été compromis. Dans certains cas, vous pouvez penser en termes de sauvegardes et d'une stratégie de reprise sur incident pour récupérer l'AD en cas de cyberattaque. Si vous êtes contraint de récupérer l'intégralité du service AD, potentiellement en tant que victime d'une attaque, rappelez-vous qu'une bonne sauvegarde de contrôleur n'est pas synonyme de récupération fluide et rapide du service AD. Il est important de s'entraîner à exécuter l'intégralité du processus de récupération périodiquement, en suivant le volumineux guide Microsoft de récupération de la forêt AD. Mais il est également important de rechercher des solutions permettant d'inverser les changements au niveau des attributs, voire de les inverser automatiquement pour protéger les objets dès la détection.

Le ciblage de l'Active Directory en vue de sa modification est une tactique répandue chez les cybercriminels modernes, à tel point que l'ancien modèle qui consistait à observer les modifications dans les événements d'audit de l'AD risque de ne plus être viable. Les organisations qui sont déterminées à assurer la sécurité et l'intégrité de leur AD doivent trouver de nouvelles solutions offrant davantage de visibilité sur toutes les modifications réalisées et permettant de les inverser ou de les récupérer si nécessaire.

Connaissez-vous les failles de sécurité de votre Active Directory ?

PAR **SEAN DEUBY,** *Director of Services chez Semperis*

La sécurisation de Microsoft Active Directory (AD) passe par le traitement de risques très divers, des erreurs de gestion aux failles de sécurité sans correctif. Nous avons souvent écrit que les cybercriminels visent l'AD pour élever leurs privilèges et s'implanter de façon persistante dans l'organisation. Menez des investigations sur une violation de données type et vous verrez que les identifiants de connexion volés peuvent être utilisés parfois pour l'entrée initiale ou parfois pour l'accès aux systèmes critiques, mais toujours au détriment de l'organisation visée.

Le renforcement de l'AD commence par la prise de mesures de réduction des vulnérabilités, ainsi que des erreurs de configuration et de gestion propices aux compromissions. Pour protéger l'AD, les administrateurs doivent comprendre comment les attaquants ciblent leur environnement. Combien d'entre eux pourraient dire immédiatement quels types de lacunes de sécurité sont exploités par les cybercriminels ?

Échec d'authentification

Cela peut sembler ironique, mais quelques-unes des erreurs de configuration les plus courantes et dommageables impactant l'Active Directory sont liées au processus d'authentification. Prenons par exemple un scénario où l'organisation doit autoriser une application tierce ou interne qui ne s'intègre pas avec l'AD, mais souhaite néanmoins rechercher les utilisateurs actifs dans l'AD. La solution la plus simple consiste à activer l'accès anonyme à l'Active Directory. Si cette mesure peut sembler plus productive du point de vue des administrateurs surchargés, elle a pour désavantage d'autoriser les utilisateurs non authentifiés à interroger l'AD. Si cette fonctionnalité est activée sans contre-mesure, le profil de risque de cette organisation va augmenter de façon significative.

La faille Zerologon signalée en 2020 a été rapidement exploitée par les attaquants, car elle leur a permis de modifier, voire de supprimer le mot de passe d'un compte de service sur un contrôleur de domaine. Les retombées d'un exploit peuvent être catastrophiques. Mots de passe faibles, mots de passe sans date d'expiration, aucun mot de passe, tous ces indices sont révélateurs d'un environnement AD non sécurisé.

Les stratégies de mots de passe sécurisés doivent être à l'ordre du jour à tous les niveaux de l'infrastructure Active Directory. Tout compte dont l'indicateur PASSWD_NOTREQD est défini représente un signal fort qui doit faire automatiquement l'objet d'une analyse plus poussée et d'une explication. D'autre part, les mots de passe, notamment ceux des comptes de service, doivent être changés périodiquement. Les mots de passe qui restent inchangés pendant des périodes prolongées augmentent le risque de succès d'une attaque par force brute, car ils restent plus longtemps exposés aux tentatives d'accès.

Principaux problèmes d'authentification à surveiller :

- Les comptes de service administré de groupe et d'ordinateurs (gMSA) ayant des mots de passe définis depuis plus de 90 jours
- Mots de passe réversibles trouvés dans les objets de stratégie de groupe (GPO)
- Accès anonyme à Active Directory activé
- Faille Zerologon (CVE-2020-1472) si le correctif n'a pas été appliqué.

Absence de contrôle des autorisations excessives

Dans la mesure où la plupart des environnements AD sont en production depuis de nombreuses années, leur surface d'attaque s'est élargie. La plupart des vulnérabilités cumulées des forêts sont dues au fait que quelqu'un doit faire faire quelque chose, généralement dans l'urgence, et que les privilèges les moins élevés prennent trop de temps pour ce faire, ne sont pas facilement accessibles ou simplement non connus. Par conséquent, l'utilisateur, le groupe ou l'autorisation utilise des privilèges trop élevés simplement pour s'assurer que la demande est satisfaite et le ticket résolu. Naturellement, ce droit n'est jamais supprimé et, par conséquent, la surface d'attaque continue de s'étendre.

En réalité, il n'est pas rare que les environnements AD aient un nombre inutilement élevé d'administrateurs de domaine, un état de fait d'autant plus troublant si ces comptes sont orphelins et risquent de servir de tremplin à la prochaine attaque. Les comptes de service ayant des autorisations excessives posent également un risque plus élevé, car non seulement leurs mots de passe n'ont pas de date d'expiration, mais ils sont aussi faibles (ce qui en fait une cible privilégiée pour le kerberoasting). Plus le nombre de privilèges d'administration augmente, plus la surface d'attaque à protéger est étendue. Les membres de ces groupes doivent être contrôlés de près.

Des erreurs peuvent se produire, cela va sans dire. Au fur et à mesure que l'environnement AD s'étend et devient plus complexe, quelqu'un peut ne pas prendre en compte correctement les autorisations héritées, par exemple, et donner par inadvertance trop de privilèges à un compte. Toutefois, une gestion correcte des privilèges n'est pas suffisante lorsque les attaquants prennent l'initiative.

Par exemple, imaginez l'impact d'une attaque AdminSDHolder. Pour mémoire, le conteneur AdminSDHolder stocke le descripteur de sécurité qui s'applique aux groupes privilégiés. Par défaut, toutes les 60 minutes, le processus SDPROP (Security Description Propagation) compare les autorisations des objets protégés, puis inverse et corrige tous les écarts en fonction de ce qui est défini dans AdminSDHolder.

En cas d'attaque AdminSDHolder, les acteurs de menaces exploitent le processus SDPROP pour assurer la persistance en remplaçant les autorisations d'un objet par les modifications non autorisées de l'attaquant. Si les modifications d'autorisations sont identifiées et annulées, alors que les modifications apportées à AdminSDHolder restent non-détectées, les changements apportés par l'attaquant seront rétablis.

Les autorisations d'audit et le monitoring des activités suspectes constituent la meilleure protection contre les abus de privilèges.

Principaux problèmes d'autorisation à surveiller :

- Objets avec privilèges appartenant à des propriétaires sans privilèges
- Modifications d'autorisations pour l'objet AdminSDHolder
- Utilisateurs sans privilèges avec des droits de synchronisation du contrôleur de données dans le domaine
- Modifications du schéma des descripteurs de sécurité par défaut au cours des 90 derniers jours

> *Pour defender AD, les administrateurs **doivent savoir comment** les attaquants ciblent leur environnement.*

SECURISER AZURE ACTIVE DIRECTORY

Principaux risques de sécurité à surveiller lors de la transition vers la gestion d'identité hybride

PAR **DOUG DAVIS,** *Senior Product Manager chez Semperis*

Il est facile de comprendre pourquoi les entreprises gravitent vers un modèle de gestion d'identité hybride qui promet de concilier le meilleur du cloud et des installations sur site. Dans un environnement tournant autour de l'Active Directory, l'exploitation des systèmes cloud se traduit par l'intégration avec Azure Active Directory.

Après tout, Azure Active Directory (AAD) est conçu en partie pour les applications SaaS, car il intègre la connexion unique (SSO) et le contrôle d'accès. La montée en puissance de l'adoption du cloud impose la gestion simultanée des accès locaux et cloud. L'exploitation conjointe de l'AAD avec l'Active Directory (AD) permet de faire de la gestion d'identité hybride une réalité.

Comme toute chose en informatique, mieux vaut bien se renseigner avant de se lancer dans l'implémentation.

Changement monumental avec déplacement dans le cloud

Le déplacement d'unités opérationnelles vers le cloud implique une adaptation. L'authentification des utilisateurs ne change pas. D'un point de vue conceptuel, les organisations doivent prendre en compte trois points essentiels.

1. Un nouveau modèle d'authentification

Après 20 ans de gestion de l'identité d'une certaine façon, l'irruption de l'AAD impose une adaptation radicale. Passer d'un usage exclusif de l'AD à l'inclusion de l'authentification cloud implique un changement d'état d'esprit et d'approche. L'AAD n'a ni unités organisationnelles, ni forêts, ni aucun objet de stratégie de groupe. Les concepts (et les leçons apprises à la dure) de sécurité des identités dans l'AD ne s'appliquent plus dans l'AAD.

De nombreux administrateurs pensent initialement que le processus de sécurisation de l'AAD est similaire à celui de l'AD, mais ce n'est pas le cas. D'autre part, vous utilisez peut-être déjà l'AAD sans le savoir. Si votre organisation exploite l'un des services cloud de Microsoft, tels qu'Office 365, AAD est déjà à l'œuvre en arrière-plan. L'AAD est également très sollicité pour se connecter à des applications SaaS autres que celles de Microsoft, telles que Salesforce. Tous ces facteurs induisent de nouvelles considérations et de nouveaux choix. Par exemple, devez-vous isoler l'AD d'AAD ou fusionner les deux avec Azure AD Connect ? Il est important de se familiariser avec de nombreux nouveaux concepts pour prendre ces décisions sans compromettre la sécurité des systèmes.

2. Extension du périmètre

Dès qu'une organisation adopte le cloud, la notion traditionnelle de périmètre réseau cesse de s'appliquer. Pour les administrateurs qui ont passé les deux dernières décennies à gérer l'AD sur site, cette notion impose un effort d'adaptation considérable. Dans un environnement d'identité hybride, les organisations doivent désormais se prémunir contre un nombre infini de points d'entrée potentiels.

3. Modifications radicales du modèle d'autorisation

L'adoption d'AAD modifie radicalement le modèle d'autorisation que les organisations doivent sécuriser. Sur site, il est relativement simple de contrôler qui dispose d'un accès physique aux contrôleurs de domaine et de manière générale les points d'entrée d'administration sont bien définis et documentés. Dans un environnement AD hybride, les identités sont désormais stockées dans le cloud et risquent donc d'être exploitées par toute personne ayant un accès Internet. Tout à coup, les administrateurs sont aux prises avec un modèle intrinsèquement ouvert pour les connexions d'accès initiales qui, lorsque vous les associez au grand nombre de services, rôles et autorisations requis, a un impact significatif sur le risque.

Microsoft a fait son possible pour préparer les entreprises aux changements induits par l'adoption d'AAD en fournissant notamment des documents de formation. Cependant, nombre de services informatiques ne mesurent pas complètement

les ramifications de la gestion d'identité hybride et si les entreprises tendent désormais à adopter une approche hybride, les attaquants ont également étendu leur mode opératoire.

En septembre 2020, les chercheurs de Mandiant (FireEye) ont relevé une augmentation du nombre d'incidents impliquant Microsoft 365 et Azure Active Directory, la plupart étant dus à des e-mails d'hameçonnage poussant les victimes à saisir leurs identifiants Office 365 sur un site d'hameçonnage. Les chercheurs de Mandiant ont également constaté l'exploitation d'un module PowerShell appelé AADInternals qui permet aux attaquants de passer de l'environnement sur site à l'AAD, de créer des backdoors, de voler des mots de passe et autres actions malveillantes. Ces menaces ne pourront que s'étendre avec la croissance exponentielle de l'intérêt pour Azure et Office 365.

Autorisations, autorisations, autorisations

De loin, parmi les trois points mentionnés ci-dessus, le principal risque de sécurité résulte des modifications apportées au modèle d'autorisation. L'adoption d'un environnement d'identité hybride donne accès à un nombre impressionnant de services. Les rôles de l'Azure Active Directory viennent se substituer à l'ensemble bien défini de groupes d'administrateurs propre à l'Active Directory, ce qui ne sera pas intuitif. Vous trouverez la liste de ces rôles ici. Chaque rôle est associé à une longue liste d'autorisations. Il est difficile de comprendre les autorisations affectées à chaque rôle uniquement à partir de la description, mais nombre d'entre elles ont un haut niveau d'accès qui n'est pas apparent.

D'autre part, la liaison d'un service SaaS à l'AAD, qui est probablement la raison pour laquelle vous avez opté pour l'AAD, ajoute des modèles d'autorisation qui doivent être gérés. Microsoft Teams, par exemple, utilise l'intégration SharePoint sur le système back end. En cas de configurations incorrectes, l'ajout d'un invité à Teams risque de créer une situation où ce nouvel utilisateur a désormais accès aux fichiers stockés sur SharePoint pour Teams. Les gens qui ont ajouté ces invités à leur canal simplement pour une discussion rapide ne se rendront pas forcément compte qu'ils ont ainsi donné accès aux fichiers SharePoint. D'autre part, la possibilité d'ajouter des applications dans Teams étend le modèle d'autorisation à ces outils tiers. Ce n'est qu'un exemple des ramifications des problèmes complexes pour chaque service géré par l'intermédiaire d'AAD.

Il est essentiel de conserver une trace des autorisations d'applications tierces et pourtant, c'est un domaine qui est insuffisamment géré par la plupart des implémentations d'AAD. Ces demandes d'autorisation ouvrent une fenêtre contextuelle à usage unique qui donne la liste des autorisations nécessaires pour l'application. Ce type de liste peut être long et doit être vérifié attentivement avant l'acceptation, mais c'est rarement le cas.

Les organisations peuvent également être confrontées à deux nouveaux scénarios en relation avec les autorisations qu'il faut faire l'effort de comprendre dans un contexte de sécurité :

- **Outils tiers qui chargent les données d'Azure AD et les stockent dans leur propre base de données.** Par exemple, une application enregistrée dans Azure AD qui permet à un système CRM de lire des profils d'utilisateurs ou qui dispose d'autres autorisations en lecture peut tout aussi bien récupérer et stocker ces données à d'autres fins. Une fois les données transférées depuis Azure AD, elles restent dans une base de données externe et l'entreprise devient dépendante du framework de sécurité de l'outil tiers.
- **Outils tiers avec un accès en écriture qui peuvent apporter des modifications en interne.** Dans ce cas, l'authentification requise pour modifier le locataire n'est plus assurée par Azure AD, mais par l'outil tiers, quelles que soient les mesures utilisées par ce dernier. Un utilisateur pourrait se connecter à cet outil sans authentification multifacteur si celui-ci ne prenait pas en charge la connexion unique (SSO), en utilisant l'application à laquelle l'autorisation est déléguée et qui réalise la procédure d'authentification en son nom sans appliquer une partie des vérifications d'usage.

Il est particulièrement souhaitable que les services informatiques limitent le nombre de personnes pouvant approuver des applications ou, tout au moins, donner des consignes claires sur les autorisations à considérer comme légitimes. L'adoption d'une approche de type identité hybride implique la mise en place d'un modèle d'autorisation beaucoup plus large. Pour ce faire efficacement, les organisations doivent établir des procédures strictes de gouvernance définissant les applications à activer et leurs droits d'accès.

Comprendre le risque de la gestion d'identité hybride

Que l'authentification se fasse dans le cloud, sur site ou les deux, la sécurité est une priorité absolue. Si la gestion de l'identité dans un environnement hybride peut sembler se résumer au déplacement d'un périphérique Windows sur AAD, ne pas prendre en compte le changement du contexte des risques ouvre la porte à des problèmes qui risquent de devenir difficiles à traiter à l'avenir. La connaissance doit toujours être la première ligne de défense, mais la quantité d'informations à assimiler pour comprendre tous les aspects d'AAD est impressionnante. Les outils natifs ou tiers qui automatisent ce processus d'apprentissage et réduisent la complexité de la sécurité permettent de réduire le risque de sécurité pendant et après le déploiement de votre environnement hybride.

NOUVELLES PERSPECTIVES SUR LA PROTECTION DES SYSTÈMES D'IDENTITÉ HYBRIDE

Par les experts de la sécurité des identités animant #HIPEurope2021

« Tout accès non autorisé à l'AD se transforme en course contre la montre. Il faut s'assurer que l'attaque ne se répand pas dans l'ensemble des forêts de l'Active Directory. Il faut analyser la violation, identifier l'impact principal et mettre en place un filet de sécurité. Il faut récupérer l'AD en quelques heures et non plus en plusieurs jours. »

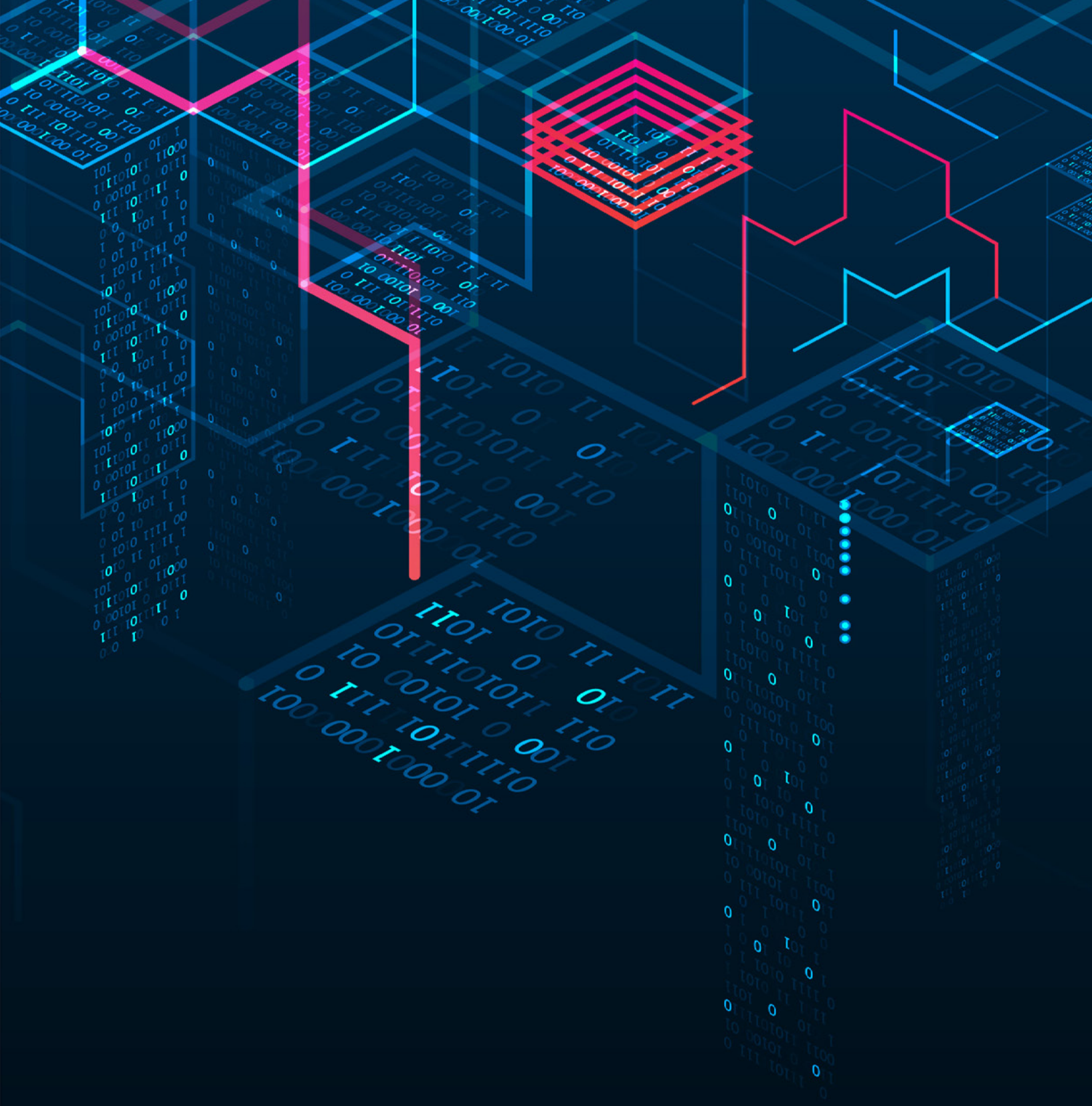
Ben Cauwel
Responsable de la sécurité chez Accenture

« L'un des principaux problèmes de la sécurité sur le cloud actuellement est que certaines personnes ne comprennent pas encore le modèle de responsabilité partagée. »

Jan de Clercq
Architecte de sécurité senior chez HPE

Pamela Dingle
Directrice des normes d'identité chez Microsoft

« À tous ceux qui n'ont pas implémenté l'authentification multifacteur : vous allez devoir redéfinir vos priorités. Vos infrastructures sur site ne sont pas à l'abri d'attaques et l'idée folle qui consiste à penser que si les utilisateurs sont sur place, on peut leur faire confiance est une véritable incitation. Les violations de la sécurité sont compliquées à gérer, coûteuses et dommageables.
Je ne dis pas que l'implémentation de l'authentification multifacteur est simple, mais que ne pas la mettre en place serait une source de problèmes sans fin. »



semperis

semperis.com