ManageEngine
ADManager Plus

Les 10 principales erreurs de configuration exposant votre Active Directory aux mouvements latéraux

Sécuriser l'infrastructure AD critique avec la GRC

www.manageengine.com/fr/ad-manager/

Introduction

Dans la plupart des environnements d'entreprise interconnectés actuels, Active Directory (AD) sert de pilier à la gestion des identités et des accès. Service central d'authentification et d'autorisation, AD contient les clés des actifs de l'entreprise, ce qui en fait une cible privilégiée des attaques.

En cas de compromission, un attaquant peut opérer des mouvements latéraux dans le réseau, élever ses privilèges et finalement obtenir un contrôle total de l'environnement. Cette technique, connue sous le nom de mouvement latéral, représente l'une des phases les plus dangereuses d'une attaque, permettant à l'attaquant d'étendre sa présence et d'accéder à des ressources de plus en plus sensibles.

Pour se protéger contre de telles menaces, l'entreprise doit dépasser les mesures de sécurité classiques et adopter une approche globale qui intègre des pratiques strictes de gouvernance, gestion des risques et conformité (GRC). Une bonne stratégie GRC garantit des contrôles d'identité et d'accès alignés sur les objectifs métier, les exigences réglementaires et les niveaux de tolérance au risque. Elle aide l'entreprise à identifier et traiter de façon proactive les erreurs de configuration, appliquer des règles cohérentes et faire preuve de la vigilance nécessaire pour protéger l'accès aux données sensibles.

Ce guide étudie les 10 principales erreurs de configuration AD qui permettent souvent un mouvement latéral. Ensuite, il expose comment ADManager Plus offre les outils nécessaires pour identifier, corriger et prévenir ces graves failles de sécurité.

L'enjeu s'avère plus élevé que jamais

Des statistiques récentes soulignent l'urgence de traiter la sécurité AD :

Le délai moyen pour déceler l'existence d'une attaque AD

peut dépasser 200 jours.

Le coût d'une violation liée aux identités atteint

4,88 millions de dollars en moyenne.

La surface d'attaque continuant à grandir avec les environnements hybrides et cloud, la sécurité de l'infrastructure AD est plus cruciale que jamais.

Analyse du mouvement latéral dans AD

Le mouvement latéral désigne les techniques qu'utilisent les attaquants pour investir progressivement un réseau après avoir obtenu un accès initial. Dans le contexte AD, le mouvement latéral consiste à exploiter des relations de confiance, des identifiants et des erreurs de configuration pour accéder à d'autres systèmes, élever les privilèges et parvenir à l'objectif visé.

Chemin d'attaque type

1. Compromission initiale :
L'attaquant pénètre dans le réseau par hameçonnage, exploitation de vulnérabilités externes ou d'autres moyens.

2. Collecte d'identifiants :
Une fois à l'intérieur, il extrait des identifiants de la mémoire, du registre ou de fichiers.

3. Élévation de privilèges :
Il utilise les identifiants collectés pour obtenir d'autres autorisations.

4. Reconnaissance du domaine :
Il cartographie la structure AD, les relations et les cibles potentielles.

5. Mouvement latéral :
Il se déplace entre les systèmes en exploitant les relations de confiance.

6. Création de persistance
Il crée des portes dérobées et d'autres méthodes d'accès.

7. Contrôle total du domaine
L'attaquant obtient un contrôle total de l'environnement AD.

Raisons de la réussite du mouvement latéral

Plusieurs facteurs courants favorisent le mouvement latéral :

- **Comptes à excès de privilèges :**
  Utilisateurs et services dotés de plus d'autorisations que nécessaire.
- **Abus de confiance :**
  Exploitation de relations de confiance mal configurées.
- **Vol d'identifiants :**
  Extraction et réutilisation d'identifiants dans l'environnement.
- **Protocoles hérités :**
  Recours à des méthodes d'authentification obsolètes et non sécurisées.
- **Lacunes de suivi :**
  Surveillance inadéquate des événements d'authentification et des modèles d'accès.

Heureusement, la plupart de ces facteurs découlent d'erreurs de configuration identifiables et corrigeables avec les bons outils et processus. ADManager Plus offre une solution complète pour découvrir et régler ces graves failles de sécurité avant qu'un attaquant ne puisse les exploiter.

10 principales erreurs de configuration AD

Erreur de configuration 1 :

Droits d'accès privilégié excessifs

Problème

L'une des erreurs de configuration AD les plus courantes et risquées est l'affectation excessive de droits d'accès privilégié. Cela comprend :

- Trop d'administrateurs de domaine.
- Appartenances à un groupe imbriquées créant des privilèges masqués.
- Accès privilégié permanent au lieu d'une affectation ponctuelle.
- Comptes de service aux privilèges d'administrateur de domaine.
- Administrateurs fantômes aux droits délégués qui octroient en fait un contrôle administratif.

Risque

Chaque compte privilégié représente un vecteur d'attaque. Une fois compromis, il donne à l'attaquant un accès direct à des ressources sensibles et lui permet de se déplacer latéralement dans l'environnement. De plus, un excès de droits viole le principe du privilège minimum et complique la conformité aux cadres réglementaires.

Erreur de configuration 2 :

Comptes de service non surveillés

Problème

Les comptes de service forment certains des objets AD les plus négligés mais dangereux. Cela comprend souvent :

- Comptes de service aux mots de passe n'expirant jamais.
- Comptes aux privilèges de domaine inutiles.
- Défaut de contrôle des liens entre les services et les comptes utilisés.
- Ni inventaire ni documentation de propriété.
- Les erreurs de configuration SPN (Service Principal Name) rendent les comptes vulnérables au Kerberoasting.

Risque

Les comptes de service ont généralement des privilèges étendus et un accès permanent. Une fois compromis, ils offrent aux attaquants un accès stable et durable aux ressources. Ces comptes exécutant souvent des services sensibles, l'activité suspecte peut rester inaperçue, car elle se mêle à des opérations légitimes.

Erreur de configuration 3 :

GPO non sécurisés

Problème

Les objets stratégie de groupe (GPO) sont de puissants outils pour gérer les configurations d'un environnement AD, mais ils présentent de sérieux risques de sécurité si on les configure mal :

- Droits de modification GPO trop permissifs.
- Paramètres de sécurité incohérents ou contradictoires.
- GPO sans lien ou orphelins.
- Stratégies d'exécution de script qui activent du code malveillant.
- Non-respect des référentiels de sécurité.

Risque

Les attaques ciblent activement les GPO, car ils offrent un moyen efficace de déployer simultanément des configurations malveillantes sur plusieurs systèmes. Un GPO compromis peut servir à désactiver des contrôles de sécurité, exécuter des scripts malveillants ou créer des portes dérobées dans l'environnement.

Erreur de configuration 4 :

Stratégies de mot de passe inadéquates

Problème

Bien qu'elles forment un contrôle de sécurité crucial, les stratégies de mots de passe restent dangereusement faibles dans nombre d'environnements AD :

- Longueurs minimales courtes des mots de passe.
- Longue durée des mots de passe, permettant le vol d'identifiants.
- Défaut d'exigences de complexité.
- Absence de règles de verrouillage des comptes.
- Application incohérente aux OU et domaines.

Risque

Les stratégies de mots de passe faibles facilitent beaucoup la compromission des identifiants. Une fois des identifiants obtenus, ils servent à accéder aux ressources, se déplacer latéralement et maintenir la persistance dans l'environnement.

Erreur de configuration 5 :

Comptes d'utilisateur et droits d'accès obsolètes

Problème

L'un des problèmes les plus courants des environnements AD réside dans l'accumulation de comptes et de droits d'accès obsolètes :

- Comptes d'anciens employés qui restent actifs.
- Comptes inutilisés mais activés.
- Droits d'accès hérités devenus inutiles.
- Accès temporaire jamais révoqué.
- SID orphelins dans les ACL.

⚠ Risque

Les comptes obsolètes et les autorisations excessives étendent la surface d'attaque et créent de possibles points d'entrée et chemins de mouvement latéral. Ces comptes présentent souvent des contrôles de sécurité et une surveillance plus faibles, ce qui en fait des cibles idéales

Erreur de configuration 6 :

Relations de domaine négligées

Problème

Les relations de confiance sont capitales pour un environnement multidomaine, mais créent souvent des risques de sécurité :

- Approbation transitive étendant l'accès au-delà des limites prévues.
- Approbation bidirectionnelle et pas à sens unique.
- Défaut de filtrage SID des relations externes.
- Relations de confiance non vérifiées.
- Approbation héritée via des fusions ou acquisitions.

⚠ Risque

Les relations de confiance créent des voies permettant à un attaquant de se déplacer entre des domaines. Mal configurées, ces relations rendent possible l'élévation de privilèges ou le mouvement latéral au-delà des limites du domaine, exposant toute la forêt à une compromission d'un seul point d'entrée.

Erreur de configuration 7 :

Mauvais contrôles de délégation

Problème

La délégation AD permet de distribuer des droits d'administration, mais une délégation incorrecte crée un risque important :

- Délégation sans contrainte à des comptes d'utilisateur ou d'ordinateur.
- Délégation excessive d'opérations sensibles.
- Défaut d'audit de délégation.
- Délégation à des groupes dont les appartenances changent.
- Mauvaise configuration de la délégation restreinte selon les ressources.

⚠ Risque

Une délégation incorrecte peut créer des portes dérobées dans des opérations privilégiées. La délégation sans contrainte est particulièrement dangereuse. Elle permet à l'objet délégué d'usurper l'identité de tout utilisateur dans n'importe quel service, aubaine pour un attaquant cherchant à élever des privilèges.

Erreur de configuration 8 :

Paramètres NTLM mal configurés

Problème

Malgré ses vulnérabilités connues, l'authentification NTLM (NT LAN Manager) reste courante dans nombre d'environnements avec des erreurs de configuration fréquentes :

- Authentification NTLM activée sans réel besoin.
- Défaut de restrictions NTLM et d'audit.
- Échec d'application de la signature NTLM.
- Paramètres de stockage de hachage LM (LAN Manager) et NTLM faibles.
- Défaut de prévention du vol d'identifiants.

⚠ Risque

Les failles NTLM permettent plusieurs techniques d'attaque, comme l'attaque par relais, de type pass-the-hash ou le vol d'identifiants. Ces vulnérabilités offrent à l'attaquant des moyens efficaces de mouvement latéral une fois le réseau pénétré.

Erreur de configuration 9 :

Contrôleurs de domaine vulnérables

Problème

Les contrôleurs de domaine sont les serveurs les plus vitaux d'un environnement AD, mais ils présentent souvent une mauvaise configuration de sécurité :

- Exécution de logiciels et de services inutiles.
- Mises à jour de sécurité et correctives manquantes.
- Faible sécurisation des systèmes.
- Accès direct inapproprié par des utilisateurs.
- Sauvegardes non protégées des systèmes.

⚠ Risque

La compromission d'un contrôleur de domaine entraîne souvent celle du domaine complet. Un attaquant visant un contrôleur de domaine peut extraire des identifiants, modifier les appartenances à un groupe, créer des comptes de porte dérobée et obtenir un accès permanent à tout l'environnement.

Erreur de configuration 10 :

Audit et surveillance inadéquats

Problème

Nombre d'entreprises ne parviennent pas à établir un audit et un contrôle adéquats de leurs environnements AD :

- Configuration de stratégies d'audit insuffisante.
- Défaut de collecte des événements de sécurité critiques.
- Absence de modèles comportementaux de base.
- Stockage et conservation de journaux inadéquats.
- Défaut d'alertes sur l'activité suspecte.

⚠ Risque

Sans bon suivi de l'activité AD, l'entreprise ne peut détecter les attaques en cours. Une attaque peut arriver sans détection, prolongeant sa durée et aggravant les dommages éventuels.

Comment les outils GRC d'ADManager Plus préviennent ces risques

ADManager Plus est une solution de gouvernance et d'administration des identités qui offre une suite complète de fonctionnalités visant spécialement à corriger les graves erreurs de configuration AD permettant le mouvement latéral. Voici cinq façons dont ADManager Plus prévient le risque de mauvaise configuration AD.

1 Certification d'accès et gestion des privilèges

Le module de certification d'accès d'ADManager Plus offre un moyen systématique de gérer et valider l'accès utilisateur :

- **Revue des accès automatique :**
  Prévoyez un controle régulier des autorisations des utilisateurs et des appartenances aux groupes.
- **Certification basée sur le risque :**
  Priorisez la revue des privilèges et des comptes à haut risque.
- **Workflows de délégation :**
  Distribuez les responsabilités de certification aux managers et propriétaires concernés.
- **Documentation de conformité :**
  Conservez des registres complets de toutes les revues et décisions d'accès.
- **Automatisation de la correction :**
  Appliquez automatiquement les modifications d'accès approuvées.

2 Analyse du chemin d'attaque

La gestion avancée des chemins d'attaque aide à comprendre et corriger les voies de mouvement latéral éventuelles :

- **Découverte du chemin d'attaque :**
  Identifiez la voie qu'un attaquant pourrait utiliser pour atteindre des actifs vitaux.
- **Visualisation du chemin :**
  Graphiques interactifs affichant les relations et le chemin de mouvement.
- **Notation du risque :**
  Priorisez les chemins selon l'exploitabilité et l'impact potentiel.
- **Conseils de correction :**
  Recommandations spéciales pour bloquer les chemins d'attaque identifiés.
- **Surveillance continue :**
  Analyse continue pour détecter de nouveaux chemins à mesure qu'évolue l'environnement.

3 Évaluation des risques complète

Le module d'évaluation des risques d'ADManager Plus permet une analyse continue de l'état de sécurité AD :

- **Analyse de la configuration de sécurité :**
  Évaluez les contrôleurs de domaine, les GPO et autres éléments sensibles.
- **Détection des vulnérabilités :**
  Identifiez les erreurs de configuration qui exposent l'environnement à une attaque.
- **Contrôle de conformité :**
  Validez les configurations par rapport aux normes et bonnes pratiques du secteur.
- **Analyse des tendances :**
  Suivez les améliorations de l'état de sécurité au fil du temps.
- **Correction prioritaire :**
  Mettez l'accent sur les lacunes de sécurité les plus graves.

4 Gestion complète du cycle de vie des utilisateurs

ADManager Plus rationalise l'affectation d'utilisateur et la révocation pour réduire les lacunes de sécurité :

- **Intégration automatisée :**
  Les nouveaux utilisateurs reçoivent un accès approprié.
- **Gestion des modifications :**
  Suivez et approuvez toutes les modifications de privilèges.
- **Workflows de départ :**
  Veillez à révoquer totalement l'accès lorsqu'un utilisateur quitte l'entreprise.
- **Revue des accès régulière :**
  Validez les besoins d'accès de tous les comptes.

Conclusion

AD reste le principal système de gestion des identités de la plupart des entreprises et continuera d'être une cible privilégiée des attaques. Les 10 principales erreurs de configuration que décrit ce guide constituent les voies les plus courantes que les attaquants exploitent pour se opérer des mouvements latéraux dans un environnement et élever des privilèges.

Les fonctionnalités avancées de certification d'accès, de gestion des chemins d'attaque et d'évaluation des risques qu'offre ADManager Plus aident à identifier et corriger ces graves vulnérabilités avant qu'un attaquant ne puisse les exploiter. En adoptant une stratégie de sécurité AD proactive étayée par les bons outils, on peut nettement réduire la surface d'attaque et protéger ses actifs les plus sensibles.

Point clé : la sécurité AD doit constituer un processus continu. Une évaluation régulière, une surveillance continue et une gestion systématique des accès sont essentielles pour maintenir une solide protection contre les menaces toujours plus sophistiquées.

ManageEngine
ADManager Plus

Nos produits

AD360 | Log360 | ADAudit Plus | ADSelfService Plus

M365 Manager Plus | RecoveryManager Plus

À propos d'ADManager Plus

ADManager Plus est une solution de gouvernance et d'administration des identités (IGA) qui simplifie la gestion des identités, renforce la sécurité et améliore la conformité. Avec ADManager Plus, gérez le cycle de vie des utilisateurs, du approvisionnement à la révocation des accès, menez des campagnes de certification des accès, orchestrez la gestion des identités à travers les applications de l'entreprise et protégez les données de vos plateformes grâce à des sauvegardes régulières. Exploitez plus de 200 rapports pour obtenir des informations précieuses sur les identités et leurs droits d'accès. Améliorez l'efficacité de vos opérations IGA grâce à des workflows, des automatisations et des politiques de contrôle d'accès basées sur les rôles (RBAC).
Les applications Android et iOS d'ADManager Plus facilitent la gestion d'Active Directory et d'Azure AD, même à distance

Pour plus d'informations sur ADManager Plus, consultez
www.manageengine.com/fr/ad-manager/

$ Obtenir un devis

Télécharger