Dix conseils pour protéger votre annuaire Active Directory

juin 8, 2022
by SentinelOne

Active Directory (AD) est une cible de choix pour les cybercriminels, qui tentent fréquemment de le compromettre dans le but d'élever leurs privilèges et d'étendre leur niveau d'accès. Cependant, en raison de sa nécessité opérationnelle, il doit être aisément accessible aux utilisateurs à l'échelle de l'entreprise – raison pour laquelle il est notoirement difficile à sécuriser. Microsoft a admis que plus de 95 millions de comptes Active Directory sont attaqués chaque jour, preuve de la gravité de la situation.

Protéger Active Directory est un défi, certes, mais il est loin d'être impossible à relever : il suffit d'opter pour les outils et tactiques appropriés. Les dix conseils ci-dessous aideront les entreprises à sécuriser plus efficacement leur infrastructure Active Directory contre les tactiques d'attaque les plus courantes.

1. Détecter et empêcher l'énumération des comptes à privilèges, des comptes d'administrateur délégué, des comptes de service et des sessions d'accès réseau

Après avoir contourné la protection périmétrique et s'être implanté dans le réseau, le cybercriminel effectue une reconnaissance pour identifier les ressources susceptibles de présenter de la valeur et déterminer comment les atteindre. Pour ce faire, il a généralement tout intérêt à cibler Active Directory, car il pourra ainsi faire passer ces opérations de reconnaissance pour des activités normales sans grand risque d'être repéré.

Un outil permettant de détecter et d'empêcher l'énumération des comptes à privilèges, des comptes d'administrateur délégué et des comptes de service peut avertir l'équipe de sécurité de la présence d'un cybercriminel au début du cycle d'attaque. En outre, le déploiement sur les endpoints de comptes de domaine et d'identifiants servant de leurres permet de duper les attaquants et de les rediriger vers des appâts destinés à les prendre au piège.

3. Identifier et corriger les expositions de comptes à privilèges

Les utilisateurs enregistrent souvent leurs identifiants sur leur poste de travail, parfois par inadvertance, parfois volontairement – généralement dans un souci de facilité. Les cybercriminels le savent et ciblent ces identifiants stockés afin d'infiltrer l'environnement réseau. Le bon jeu d'identifiants peut être une carte maîtresse pour un intrus, qui cherche toujours à étendre ses privilèges et son niveau d'accès.

Pour éviter de laisser le champ libre aux attaquants, les entreprises peuvent prendre diverses mesures, comme identifier l'exposition des comptes à privilèges, corriger les problèmes de configuration ou encore supprimer les identifiants enregistrés, les dossiers partagés et d'autres vulnérabilités.

3. Détecter et neutraliser les attaques par « Golden Ticket » et « Silver Ticket »

Les attaques de type Pass-The-Ticket (PTT) comptent parmi les techniques les plus avancées auxquelles les cybercriminels ont recours pour se déplacer latéralement dans un réseau et élever leurs privilèges. Kerberos étant par nature sans état (stateless), il est facile à exploiter et permet aux cybercriminels de falsifier sans grande difficulté des tickets au sein du système. Particulièrement redoutables, deux techniques PPT appelées « Golden Ticket » et « Silver Ticket » sont utilisées pour compromettre un domaine et s'y établir de manière persistante.

Pour les contrer, il est nécessaire de disposer d'un outil capable de détecter les comptes de service et les comptes TGT (Ticket Granting Ticket) vulnérables Kerberos, pour identifier et signaler les erreurs de configuration susceptibles de conduire à des attaques PTT. De plus, une solution telle que Singularity Identity peut empêcher l'emploi de tickets falsifiés au niveau des endpoints.

4. Se prémunir contre les attaques Kerberoasting, DCSync et DCShadow

Une attaque Kerberoasting offre aux cybercriminels une méthode simple pour obtenir un accès à privilèges, tandis que les techniques DCSync et DCShadow leur permettent d'établir leur persistance sur un domaine au sein de l'entreprise prise pour cible.

Les responsables de la cybersécurité doivent pouvoir soumettre Active Directory à une évaluation continue qui analyse en temps réel les attaques dont il fait l'objet, tout en épinglant les problèmes de configuration ouvrant la voie à ces attaques. En outre, une solution présente au niveau de l'endpoint pour empêcher la découverte de comptes à cibler peut freiner les tentatives d'intrusion.

5. Prévenir la collecte d'identifiants à partir des partages de domaine

Les cybercriminels ciblent généralement les mots de passe stockés en clair ou de manière réversible dans des scripts ou fichiers de stratégie de groupe enregistrés dans des partages de domaine tels que Sysvol ou Netlogon.

Une solution telle que Ranger AD permet de détecter ces mots de passe, offrant aux responsables de la sécurité la possibilité d'éliminer les expositions avant qu'un attaquant ne puisse en tirer parti. Des mécanismes comme ceux offerts par la solution Singularity Identity sont également utiles pour déployer des objets stratégie de groupe Sysvol servant de leurre dans l'annuaire Active Directory de production, de façon à détourner l'intrus des ressources de production pour mieux le déstabiliser.

6. Identifier les comptes avec SID à privilèges caché

La technique d'injection de valeurs SID (identificateur de sécurité) Windows permet aux cybercriminels d'exploiter l'attribut SID History pour se déplacer latéralement dans l'environnement Active Directory et se doter de privilèges plus élevés.

Une mesure de prévention consiste à détecter et à signaler les comptes comportant des valeurs SID à privilèges connues au niveau de leur attribut SID History.

7. Détecter les pratiques dangereuses de délégation de droits d'accès sur les objets critiques

La délégation est une fonctionnalité d'Active Directory qui autorise un compte d'utilisateur ou d'ordinateur à agir au nom d'un autre compte. Par exemple, lorsqu'un utilisateur appelle une application Web hébergée sur un serveur Web, l'application peut reproduire les identifiants de l'utilisateur pour accéder à des ressources hébergées sur un autre serveur. Tout ordinateur de domaine bénéficiant d'une délégation sans contraintes peut emprunter l'identité d'un utilisateur (c'est-à-dire utiliser ses identifiants) pour communiquer avec tout autre service de ce même domaine. Malheureusement, les cybercriminels peuvent exploiter cette fonctionnalité pour accéder à différentes zones du réseau.

La surveillance permanente des vulnérabilités d'Active Directory et des expositions en matière de délégation peut aider les équipes de sécurité à identifier et à corriger ces failles avant que les cybercriminels ne puissent en profiter.

8. Identifier les comptes à privilèges dont la délégation est activée

Les comptes à privilèges configurés avec la délégation sans contraintes peuvent être à l'origine d'attaques Kerberoasting et par Silver Ticket. La détection et le signalement des comptes à privilèges dont la délégation est activée sont indispensables pour les entreprises.

Une liste complète des comptes d'utilisateur à privilèges, des comptes d'administrateurs délégués et des comptes de service peut contribuer au recensement des vulnérabilités par les responsables de la sécurité. La délégation n'est pas nécessairement mal venue. Elle est souvent nécessaire pour des raisons opérationnelles, et les équipes de sécurité peuvent recourir à un outil tel que Singularity Identity pour empêcher les cybercriminels d'identifier les comptes à cibler.

9. Identifier les utilisateurs sans privilèges présents dans la liste de contrôle d'accès d'AdminSDHolder

Les Services de domaine Active Directory (AD DS) utilisent l'objet AdminSDHolder et le processus de propagateur de descripteurs de sécurité (SDProp) pour sécuriser les comptes d'utilisateur et de groupe à privilèges. L'objet AdminSDHolder dispose d'une liste de contrôle d'accès (ACL) unique qui contrôle les autorisations des principaux de sécurité membres des groupes à privilèges prédéfinis dans Active Directory. Pour pouvoir se déplacer latéralement, les cybercriminels peuvent ajouter des comptes à l'objet AdminSDHolder et leur accorder les mêmes privilèges d'accès que ceux des autres comptes protégés.

Les entreprises peuvent les en empêcher grâce à un outil comme Ranger AD, qui détecte et signale la présence de comptes inhabituels dans la liste de contrôle d'accès d'AdminSDHolder.

10. Identifier les modifications récentes à la stratégie de domaine par défaut ou à la stratégie des contrôleurs de domaine par défaut

Dans Active Directory, une organisation utilise des stratégies de groupe pour gérer plusieurs configurations opérationnelles en définissant des paramètres de sécurité propres à l'environnement. Bien souvent, ces stratégies servent à configurer des groupes d'administration, et contiennent des scripts de démarrage et d'arrêt. Les administrateurs y définissent les exigences de sécurité fixées par l'organisation à chaque niveau, les modalités d'installation des logiciels ainsi que les autorisations sur les fichiers et le Registre. Les cybercriminels peuvent toutefois modifier ces stratégies de manière à maintenir leur persistance sur le domaine compromis au sein du réseau.

La surveillance des modifications apportées aux stratégies de groupe par défaut peut aider les équipes de sécurité à repérer rapidement ces intrus, afin d'atténuer les risques et d'empêcher l'accès avec privilèges à Active Directory.

Mettre en place les outils appropriés

Connaître les tactiques que les cybercriminels privilégient pour cibler Active Directory peut aider les entreprises à en assurer la protection. Lors du développement d'outils tels que Ranger AD et Singularity Identity, nous avons étudié de nombreux vecteurs d'attaque et déterminé les meilleures stratégies pour les détecter et les neutraliser.

Une fois dotées de ces outils, les entreprises sont à même d'identifier avec précision les vulnérabilités, de détecter les activités malveillantes sans délai et de remédier aux incidents de sécurité avant que des intrus ne puissent prendre les commandes et transformer une attaque de faible ampleur à une compromission majeure. Le défi que représente la protection d'Active Directory n'est pas insurmontable, grâce aux outils dédiés disponibles aujourd'hui.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- Sécurité d'Active Directory | Ce qu'il faut savoir