PARTENAIRES

Ma page de départ sécurisée

UserLock

GUARDIA RÈGLES DE CYBERSÉCURITÉ

ZATAZ PARTENAIRE INCYBER FORUM EUROPE

ProtonVPN PROTÈGES VOS MAILS ET CONNEXIONS WEB !

Stoppez les déplacements latéraux grâce à la sécurité des accès Zero Trust

Posted On 27 Nov 2024 By : Auteur exterieur Comments: 2 Tag: sécurité d'Active Directory

Les déplacements latéraux posent un risque considérable pour la sécurité d'Active Directory (AD). Les attaquants tentent de se déplacer latéralement à l'intérieur des réseaux pour relever leur niveau de privilège et étendre leur accès afin de pouvoir exécuter du code à distance et d'explorer le réseau sans se faire remarquer.

Voici comment l'authentification multifacteur (MFA) et les contrôles d'accès contribuent à stopper les déplacements latéraux liés aux menaces les plus courantes basées sur les identités, qui concernent tous les utilisateurs, et pas seulement les comptes privilégiés.

Comprendre les déplacements latéraux au sein d'Active Directory

Abordons un instant la question des déplacements latéraux et de leurs implications vis-à-vis de la sécurité d'Active Directory.

En quoi consistent les mouvements latéraux ?

On désigne par l'expression « déplacement latéral » les différentes techniques utilisées par les cybercriminels pour pénétrer de façon progressive au sein d'un réseau en vue d'y rechercher des données et des ressources de valeur. Après l'accès initial, généralement via un endpoint faible ou compromis, l'attaquant parcourt le réseau en passant d'un système à l'autre.

Les déplacements latéraux aident les acteurs malveillants à exercer toute détection et à maintenir leur accès aux systèmes, même si la faille initiale a été détectée. Le vol de données peut se produire plusieurs semaines, voire plusieurs mois après la faille initiale.

En moyenne, il faut 210 jours pour identifier une faille.

En se faisant passer pour un utilisateur légitime, le criminel collecte des informations sur les systèmes et les comptes, récupère des identifiants, relève son niveau de privilège et finit par accéder à la cible identifiée. La Confiance Zéro (Zero Trust) appliquée aux accès et la gestion des accès privilégiés contribuent à empêcher les déplacements latéraux.

Risques liés aux déplacements latéraux

Un déplacement latéral indique qu'un attaquant a infiltré les défenses externes de l'entreprise et opère librement au sein du réseau. Les risques associés à une telle infiltration sont importants.

Pertes financières

Le vol de propriété intellectuelle (IP) peut conduire à une perte d'avantage concurrentiel et de futures sources de revenus.

Les coûts associés aux efforts de remédiation peuvent grimper : investigation numérique, restauration des systèmes ou encore paiement d'une rançon.

À prendre en compte également, les coûts liés au signalement de l'incident aux parties affectées et la mise en place de services de suivi des crédits en cas de fuite de données.

Préjudice en termes d'image

Une publicité négative immédiate peut entraîner une dépréciation rapide du cours en bourse des entreprises cotées.

La perte de confiance auprès des clients réduit le volume des ventes et complique la fidélisation de la clientèle.

Le préjudice en termes d'image peut persister longtemps après l'incident et assombrir les perspectives de développement de l'entreprise.

Ensemble, ces risques soulignent à quel point il est important de bien identifier et empêcher les déplacements latéraux.

Techniques courantes utilisées pour le déplacement latéral

Les cybercriminels ont recours à différentes techniques pour se déplacer latéralement et relever leur niveau de privilège :

Reconnaissance LDAP : générer des requêtes auprès des services d'annuaire en vue de cartographier les cibles à forte valeur.

Attaques Pass-the-Hash : voler le mot de passe d'utilisateurs privilégiés par interception réseau ou malware.

Kerberoasting : exploiter Kerberos pour voler les identifiants d'un compte de service.

Exploiter les configurations vulnérables : profiter des systèmes mal configurés.

Exploiter le protocole RDP : utiliser les outils de bureau distant pour accéder à plusieurs systèmes.

Mise en œuvre de la MFA pour empêcher les déplacements latéraux

L'authentification multifacteur (MFA) représente une mesure de riposte contre les tentatives de déplacement latéral.

Pourquoi la MFA est cruciale pour empêcher les déplacements latéraux

Un déplacement latéral commence généralement par une compromission d'identifiants non-administrateur. La MFA stoppe l'infiltration initiale en ajoutant une couche de sécurité supplémentaire aux combinaisons nom d'utilisateur/mot de passe.

Outre le fait qu'elle stoppe les tentatives de connexion abusives, la MFA évite également que les attaquants (ou les auteurs de menaces internes) exploitent un accès non autorisé à Active Directory. Elle les empêche de se déplacer sur le réseau, d'élever leurs privilèges, de déployer des ransomwares ou des malwares et de voler des données.

Renforcez les contrôles d'accès pour éviter les déplacements latéraux

Si la MFA est précieuse pour éviter les déplacements latéraux, elle n'est pas le seul outil à votre disposition. En associant la MFA à d'autres contrôles des accès, vous renforcez la sécurité d'Active Directory contre toutes les menaces, externes comme internes. Voici les moyens les plus courants pour y parvenir.

Appliquez le principe du moindre privilège

Selon le principe du moindre privilège (ou PoLP), les utilisateurs ou les entités doivent uniquement avoir accès aux données, ressources et applications spécifiques dont elles ont besoin pour accomplir leur travail.

L'application du PoLP réduit la surface d'attaque et le risque de propagation des malwares, ainsi que les déplacements latéraux. Le PoLP fait partie des fondements du modèle Zero Trust, qui permet un contrôle extrêmement fin des accès en s'appuyant sur l'identification précise des applications et des fonctions spécifiques accessibles via l'ensemble des ports et protocoles.

Ce principe dispense les administrateurs de réfléchir en termes de blocs réseau et permet d'appliquer de façon rigoureuse un accès basé sur le moindre privilège.

Utilisez le contrôle d'accès basé sur les rôles (RBAC)

Le contrôle d'accès basé sur les rôles (RBAC) attribue des permissions aux utilisateurs en fonction de leur rôle dans l'organisation. La gestion des accès devient plus facile et moins sujette aux erreurs (et plus rapide) que lorsqu'il s'agit de gérer les permissions de chaque utilisateur.

L'approche RBAC regroupe les utilisateurs en rôles en fonction de leurs responsabilités communes et attribue des permissions à ces rôles. Les relations utilisateur-rôle et rôle-permission simplifient la gestion des utilisateurs en pilotant les privilèges à l'aide des permissions de rôle plutôt qu'individuellement.

Gestion des accès privilégiés

Un système de gestion des accès privilégiés (PAM) contrôle les accès et les permissions à niveau élevé de privilège dans tout l'environnement IT. La bonne configuration des contrôles d'accès privilégiés à l'aide d'un système de PAM réduit la surface d'attaque au minimum et stoppe les déplacements latéraux en atténuant l'impact potentiel des menaces externes et internes.

L'application du principe de moindre privilège est fondamentale pour la PAM. Il restreint les droits d'accès et les permissions des utilisateurs, des comptes, des applications, des systèmes, des machines et des processus au strict minimum nécessaire pour les activités autorisées.

Exemples réels et bonnes pratiques

Une faille récente ayant fait les gros titres a montré les conséquences d'une mauvaise configuration des contrôles de sécurité et l'importance de bien suivre les bonnes pratiques.

Faille Change Healthcare

Au mois de février dernier, le groupe de ransomware ALPHV/BlackCat a infiltré l'entreprise Change Healthcare, où il a perturbé les opérations, volé 4 To de données sensibles et perçu une rançon de 22 millions de dollars. Change Healthcare, qui traite chaque année 15 milliards de transactions de santé pour une valeur de 1 500 milliards de dollars, a dû fermer certains sites critiques et a rencontré des difficultés pour remettre ses systèmes en ligne.

Le 12 février, BlackCat a utilisé des identifiants compromis pour accéder à un portail Citrix de Change Healthcare sur lequel l'authentification multifacteur n'avait pas été déployée. Neuf jours plus tard, après s'être déplacé latéralement dans l'environnement pour en exfiltrer des données, le groupe a déployé un ransomware qui a chiffré les systèmes de Change, les rendant inaccessibles.

Une enquête de l'American Medical Association, plus importante association de médecins et d'étudiants en médecine aux États-Unis, a conclu que 80 % des gérants d'établissements de santé avaient subi des pertes financières à cause de cette faille, et que 77 % d'entre eux avaient connu des perturbations de service. 55 % des propriétaires de cabinets médicaux ont dû utiliser leurs fonds personnels pour payer leurs factures et leurs employés. D'autres praticiens se sont retrouvés dans l'incapacité d'approuver des ordonnances ou des interventions.

Bonnes pratiques pour la surveillance et la détection des déplacements latéraux

Passons en revue quelques bonnes pratiques de sécurité IT qui aideront les entreprises à détecter et à empêcher les déplacements latéraux.

Choisissez des outils associant sécurité et visibilité : Traquez les actions des administrateurs et appliquer la MFA sur les événements UAC (invites UAC et demandes « Exécuter en tant qu'administrateur »). Vous bénéficiez ainsi d'une meilleure visibilité sur les tentatives d'accès aux comptes administrateurs, les actions privilégiées et les demandes d'élévation des privilèges sur l'ensemble du réseau. Il vous suffit de définir des politiques de MFA spécifiques pour ces demandes, en précisant leur fréquence et les conditions d'application.

Auditez votre hygiène de sécurité : Vérifiez que les fondamentaux de la sécurité réseau sont appliqués de façon homogène à l'ensemble des utilisateurs, applications, réseaux et endpoints afin de maintenir une posture de sécurité robuste et d'empêcher les déplacements latéraux.

Utilisez la segmentation réseau : Segmentez le réseau à l'aide de contrôles d'accès et de pare-feu pour limiter les déplacements latéraux entre les différents segments et réduire les possibilités de progression des attaquants.

Tenez-vous informé de l'actualité des renseignements sur les menaces et les indicateurs de compromission (IOC) : Restez au fait de l'actualité des renseignements sur les menaces et les indicateurs de compromission (IOC) pour mieux identifier les techniques de déplacement latéral connues et renforcer vos capacités de détection.

Votre feuille de route vers une sécurité réseau plus robuste

Un modèle de sécurité ZeroTrust favorise la mise en place de mesures de sécurité qui empêchent tout déplacement latéral. Ces mesures incluent le principe du moindre privilège, l'audit des pratiques de sécurité, l'implémentation de la MFA, les mots de passe forts et la création de politiques communes. Si elles sont déployées ensemble, les intrus peineront à accéder au réseau et à se déplacer à l'intérieur de celui-ci.

L'adoption d'une stratégie d'accès Zero Trust sera d'autant plus efficace que les contrôles d'accès et la gestion des privilèges seront granulaires, pour une approche complète permettant de stopper les déplacements latéraux et de protéger l'entreprise des menaces basées sur les identités.

Au sujet de l'auteur
Auteur Extérieur.

« Previous Story
Molotov alerte ses utilisateurs après une intrusion dans ses systèmes

Next Story »
Mikhail Malyew : le « roi des ransomwares » jugé en Russie

2 Comments

Noname *28/01/2024 at 05:57*

Je trouve que l'article a été un peu bâclé. Les idées sont là mais il y a beaucoup trop de raccourci et certaines précisions ont été omise ce que rend l'article moins « attrayant ». Une relecture permettrait de corriger les passages problématiques, c'est assez dommage car j'avais personnellement érigé ce site comme un source fiable et intarissable en termes de culture cyber…

Damien Bancal *01/12/2024 at 11:08*

Bonjour.
Merci pour votre retour.
Il aurait été appréciable que vous nous indiquiez ce que vous avez trouvé « bâclé ». Nous alertons l'auteur et lui proposons de le mettre à jour. N'oubliez pas que nous souhaitons un contenu accessible à toutes et tous, donc compréhensible à toutes et tous.

Belle journée

PARTENAIRES DE ZATAZ

Le coffre-fort numérique certifié CSPN par l'ANSSI
Découvrez Lockbyte!

LES CYBERMENACES PEUVENT VENIR DE N'IMPORTE OÙ. BARRACUDA VOUS PROTÈGE PARTOUT.
Découvrez

MERCI !
ZATAZ CLASSÉ 9e INFLUENCEUR CYBER D'EUROPE !

SERVICE VEILLE ZATAZ
DÉCOUVRIR !

ZATAZ Réseaux Sociaux
YOUTUBE
TWITTER
INSTAGRAM
TIKTOK
TWITCH
FACEBOOK

PUBLICITÉ

PUBLICITÉS

RECHERCHER UNE INFO

OPTIMISÉ PAR Google
Rechercher

CALENDRIER

mars 2025

L	M	M	J	V	S	D
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

« Fév

LES + COMMENTÉS

Retour du chantage par mail : je vous vois à poil !
210 Comments

Escroquerie : chantage par mail à l'encontre de milliers de Français
206 Comments

Chantage par mail : NON vous n'avez pas été piraté
150 Comments

PUBLICITÉS

DATA SECURITY

- Root écope de 900 000 € d'amende pour avoir exposé les données de 45 000 clients 27/03/2025
- Violation massive de données à la Pennsylvania State Education Association plus de 500 000 personnes affectées 27/03/2025
- Cybertattaque sur le bureau du procureur général de Virginie : le groupe Cloak revendique la responsabilité 27/03/2025
- Rakuten face à une vague d'escroqueries par hameçonnage : les clients appelés à renforcer leur sécurité 27/03/2025
- Chrome sous attaque : une faille critique exploitée dans une campagne de cyber espionnage 27/03/2025
- Prison ferme requise contre une vendeuse de téléphones Enorochat 25/03/2025
- La Chine dévoile un puissant coupe-câble sous-marin : un bouleversement potentiel de l'ordre mondial 25/03/2025
- Le Trésor américain lève les sanctions contre Tornado Cash 25/03/2025
- DollyWay : la menace invisible qui frappe WordPress depuis 2016 25/03/2025
- La justice annule la condamnation de Paige Thompson pour le piratage de Capital One 20/03/2025
- Immersive World : la création de malwares voleurs de mots de passe via l'IA 20/03/2025
- Microsoft coupe les ponts : Huawei bascule sur HarmonyOS et Linux 20/03/2025
- Créer un inventaire des actifs d'IA : une nécessité stratégique pour la sécurité et la conformité 17/03/2025
- Un outil gratuit pour vaincre le ransomware Akira sur Linux 17/03/2025
- Mora_001 : un nouveau ransomware exploite des failles Fortinet 17/03/2025
- La cybercriminalité en France en 2024 : analyse des 348 000 infractions enregistrées 17/03/2025
- DeepSeek : 12 000 Clés API Exposées — L'IA, nouvelle faille de sécurité ? 10/03/2025

Copyright 1996 - 2020 : ZATAZ - Réalisation DB. - Le site OFFICIEL est ZATAZ.COM - Le reste ne serait que contrefaçon

Paramètres concernant la confidentialité et les cookies
Géré par Google. Conforme au TCF de l'IAB. ID de CMP : 300