Devolutions

Conseils de sécurité : combler le fossé entre l'authentification et l'autorisation

LA « JOURNÉE DE LA GESTION DES IDENTITÉS »

Le deuxième mardi du mois d'avril souligne la « Journée de la gestion des identités ». Créée par l'Identity Defined Security Alliance (IDSA), cette journée spéciale sera officiellement inaugurée cette année. Ce sera l'occasion d'éduquer les dirigeants d'entreprise et les décideurs informatiques sur l'importance de la gestion des identités et des composantes clés qui en font partie, dont la gouvernance, les bonnes pratiques, les processus et la technologie.

Bien qu'on accorde de l'attention à cet enjeu depuis plusieurs années (après tout, les pirates informatiques font partie du paysage numérique depuis des décennies), il est aujourd'hui plus crucial que jamais. Les chiffres parlent d'eux-mêmes :

- 74 % des violations de données découlent d'une utilisation abusive d'informations d'identification privilégiées.
- 65 % des entreprises ont plus de 1 000 comptes utilisateurs périmés.
- Le mot de passe le plus populaire en 2020 est « 123456 ». Il a été utilisé par plus de 2,5 millions de personnes et apparaît plus de 23 millions de fois dans des fuites de données.

En théorie, la gestion des identités est essentielle pour toutes les entreprises. En pratique, c'est plus compliqué que ça. Pour y voir plus clair, prenons d'abord un peu de recul et examinons deux fonctions liées, mais distinctes : **la gestion des identités et la gestion des accès.**

La gestion des identités

La gestion des identités, ça consiste à combiner des éléments numériques et des entrées au sein d'une base de données centralisée pour créer une désignation unique à chaque utilisateur. Ces désignations sont ensuite surveillées, ajustées ou supprimées (si nécessaire) afin de renforcer la sécurité. Tout ça en fournissant aux utilisateurs les autorisations nécessaires pour qu'ils puissent travailler efficacement au quotidien.

La gestion des accès

La gestion des accès détermine si les utilisateurs sont autorisés ou non à accéder à certaines ressources, applications, bases de données, zones du réseau, etc. Elle englobe toutes les politiques, processus, méthodes, systèmes et outils qui contiennent des accès privilégiés au sein d'un environnement numérique.

Authentification vs autorisation

Les deux fonctions sont conçues pour augmenter la productivité des utilisateurs et soutenir des programmes de sécurité de l'information performants. Ce n'est donc pas par hasard qu'on observe un chevauchement entre la gestion des identités et la gestion des accès. D'ailleurs, plusieurs articles les traitent comme étant la même chose. C'est pourquoi la majorité du grand public croit qu'il s'agit de synonymes.

Alors, comment les différencier? La gestion des identités concerne l'authentification (l'utilisateur) tandis que la gestion des accès concerne l'autorisation (ce à quoi un utilisateur authentifié peut accéder).

Améliorer la gestion des identités : tout un défi

Un des principes de la gestion des identités consiste à établir une source faisant autorité sur les données d'identité fiables (c'est-à-dire des attributs d'authentification et des attributs d'abonné). Par contre, encore à ce jour, les technologies comme certains équipements réseau, systèmes hérités, téléphones et caméras ne peuvent pas utiliser un système fédéré. Et même s'il est théoriquement possible de créer et de gérer manuellement des comptes d'identité uniques pour chaque utilisateur d'une entreprise, ce n'est tout simplement pas faisable dans la vraie vie. On ne parle pas ici d'un effort colossal, mais bien herculéen!

Des comptes partagés sont parfois nécessaires

Pour compliquer les choses, de nombreuses entreprises ont besoin de comptes partagés (c'est-à-dire privilégiés) pour effectuer certaines activités. Parmi ceux-ci, on retrouve :

- Les **comptes administrateur de domaine**
- Les **comptes administrateur locaux**
- Les **comptes d'accès d'urgence**
- Les **comptes d'applications**
- Les **comptes système**
- Les **comptes de services de domaine**

Avec les comptes partagés, l'identité n'est pas exclusivement associée à un utilisateur spécifique. Elle est plutôt associée à un rôle, une équipe ou un groupe.

Dans ce cas, comment les entreprises peuvent-elles trouver une façon à la fois pratique et durable de combler le fossé entre la gestion des identités (authentification) et la gestion des accès (autorisation)?

La solution : **implanter un système de gestion d'accès privilégiés** (de l'anglais *Privileged Access Management*, **PAM**).

Pourquoi un système PAM?

Grâce à leurs nombreuses fonctionnalités, les systèmes PAM utilisent le contrôle d'accès basé sur les rôles pour agir en tant que gardien des comptes partagés, tout en ajoutant une couche non négligeable de surveillance et d'audit des comptes privilégiés. Parmi ces fonctionnalités, on retrouve :

- Un **coffre sécurisé** qui stocke les informations d'identification et autres données sensibles qui doivent être partagées entre plusieurs utilisateurs (par exemple, les clés de licence logicielle, etc.).
- La **détection de comptes**, qui analyse et détecte automatiquement les comptes privilégiés d'un répertoire Active Directory (plus d'informations ci-dessous).
- La **demande de réservation de compte**, qui notifie les administrateurs système et leur permet d'approuver ou de rejeter la demande au cas par cas (dans le cas des approbations, vous devriez définir une limite de temps d'accès pour éviter que les comptes privilégiés soient laissés sans surveillance).
- La **réinitialisation automatique des mots de passe** lors de la restitution du compte.

PAM et détection de comptes

Une recherche a révélé que 88 % des entreprises ayant plus d'un million de dossiers n'ont pas de limites d'accès appropriées et 58 % d'entre elles ont plus de 100 000 dossiers accessibles à tous leurs employés. La fonction de détection de comptes d'un système PAM identifie les comptes privilégiés pour les mettre à jour, les surveiller ou les supprimer. À l'inverse, les fournisseurs d'identification comme les systèmes de gestion des identités et des accès (IAM), les bases de données, l'équipement réseau et les serveurs doivent être interrogés pour découvrir les comptes.

Gestion des sessions privilégiées

Les systèmes PAM les plus sophistiqués prennent également en charge la gestion de sessions privilégiées (PSM ou *Privileged Session Management*). Il s'agit d'un outil complémentaire qui utilise un **serveur spécialisé pour assurer l'authentification en arrière-plan, tout en enregistrant l'activité des sessions à distance**. La gestion de sessions privilégiées est particulièrement importante pour les entreprises faisant affaire avec des sous-traitants ou des employés « boomerang » (c'est-à-dire des employés qui quittent l'entreprise et y reviennent fréquemment). Ces utilisateurs ont généralement besoin d'une surveillance plus approfondie et d'un accès limité.

Comptes doubles

Les entreprises devraient créer des comptes doubles pour leurs utilisateurs disposant des privilèges les plus élevés. Ainsi, le premier compte possède un accès relativement limité, destiné uniquement aux tâches quotidiennes. Le deuxième compte possède des accès plus étendus pour effectuer les tâches administratives. Évidemment, le deuxième compte doit être géré par le système PAM et configuré selon une sécurité renforcée (comme l'injection d'identifiants obligatoire et la rotation des mots de passe après utilisation).

En résumé

Dans un monde idéal, les entreprises utiliseraient une seule identité pour tout. Sauf que dans la vraie vie, les choses sont plus compliquées - et plus difficiles! Pour freiner les pirates et limiter les abus, il faut que les entreprises puissent combler le fossé entre les authentifications et les autorisations. Et tout ce travail ne devrait pas seulement être la priorité des grandes entreprises. La preuve : 43 % des cyberattaques **visent des PME**. Le coût moyen d'une seule violation a dépassé les 200 000 $ - ce qui est plus que suffisant pour mettre en faillite plusieurs petites entreprises.

Un système PAM atteint son objectif de protection des ressources et des comptes quand **l'accès des utilisateurs ne peut pas être fédéré**. En intégrant un système PAM à un IAM et en le personnalisant avec des alertes et un processus d'approbation, les entreprises ont alors une visibilité totale sur leurs infrastructures. C'est une étape importante – voire obligatoire – vers une **meilleure protection des données et une meilleure application de la conformité, tout en permettant aux utilisateurs de travailler efficacement.**