LIVRE BLANC | MAI 2017

Modèle de maturité de la gestion des accès à forts privilèges pour la transformation numérique et l'automatisation à l'échelle de votre entreprise

ca technologies

Table des matières

Résumé

Défi

Les organisations engagées dans un processus de transformation numérique sont davantage préoccupées par des questions liées au risque et à la sécurité, ce qui n'a rien de surprenant. Les initiatives de transformation numérique entraînent inévitablement une augmentation du nombre de points d'accès à l'infrastructure de l'entreprise qui se situent en dehors des contrôles existants et sont accessibles par des identités plus nombreuses et plus variées qui prolifèrent à l'intérieur d'une infrastructure distribuée et dynamique.

Solution

Connaître vos utilisateurs privilégiés, c'est connaître vos risques. Les outils de gestion des accès à forts privilèges doivent eux-mêmes être en mesure de supporter l'automatisation du processus d'autorisation et permettre l'évolutivité grâce à la prise en charge des opérations dynamiques et de l'infrastructure éphémère, comme les comptes d'administration AWS (Amazon Web Services) pour les identités humaines.

Avantages

Une meilleure identification des attaques exploitant des informations d'identification n'est pas qu'une question d'accumulation de données. Il s'agit d'intégrer des données plus pertinentes sur le comportement des utilisateurs à forts privilèges, car celles-ci permettent d'identifier les modifications importantes représentant un véritable risque. Cette approche est renforcée via l'intégration de systèmes de gouvernance des accès à forts privilèges pour permettre d'analyser le comportement des utilisateurs ayant des rôles similaires.

Section 1

Introduction

Les logiciels sont désormais essentiels au bon fonctionnement et à la compétitivité des entreprises du XXIe siècle. La technologie joue depuis longtemps un rôle central dans la stratégie métier. Cependant, avec la transformation numérique, les initiatives de transformation et d'accélération du cycle de livraison logicielle et des processus de développement des applications sont devenues un impératif touchant l'ensemble de l'entreprise et qui, de surcroît, rejoint de plus en plus une autre inquiétude des équipes de direction : la cybersécurité.

La transformation implique inévitablement des changements et, par extension, des risques. Alors que les entreprises progressent dans leur transformation numérique, le risque s'intensifie, à moins qu'elles n'aient élaboré un plan pour la gouvernance et la sécurité des accès évoluant en parallèle avec leurs initiatives et reflétant les priorités de nombreux plans de transformation numérique :

- La facilitation d'une automatisation axée sur la responsabilisation et la visibilité
- Le développement d'une rapidité de livraison qui va de pair avec la protection des ressources de l'entreprise
- La mise à l'échelle avec l'intégration de la gouvernance des accès et de la détection des menaces

Garantir la visibilité et la responsabilisation à des fins de conformité, de sécurité et de gouvernance tout en assurant la flexibilité nécessaire à la transformation numérique demande une approche nouvelle et cohérente pour définir les personnes, mais aussi les « choses » (applications, services, machines et autres) qui reçoivent les clés du royaume, à savoir les accès à forts privilèges.

De la même façon que les entreprises s'engagent désormais à définir un plan d'action pratique pour leur transformation numérique, les équipes de sécurité doivent disposer des bons outils et des capacités d'intégration adéquates pour progressivement automatiser, accélérer et mettre à l'échelle la gestion des accès ainsi que l'atténuation des risques en accord avec les besoins métier, et ce à moindre coût.

Section 2

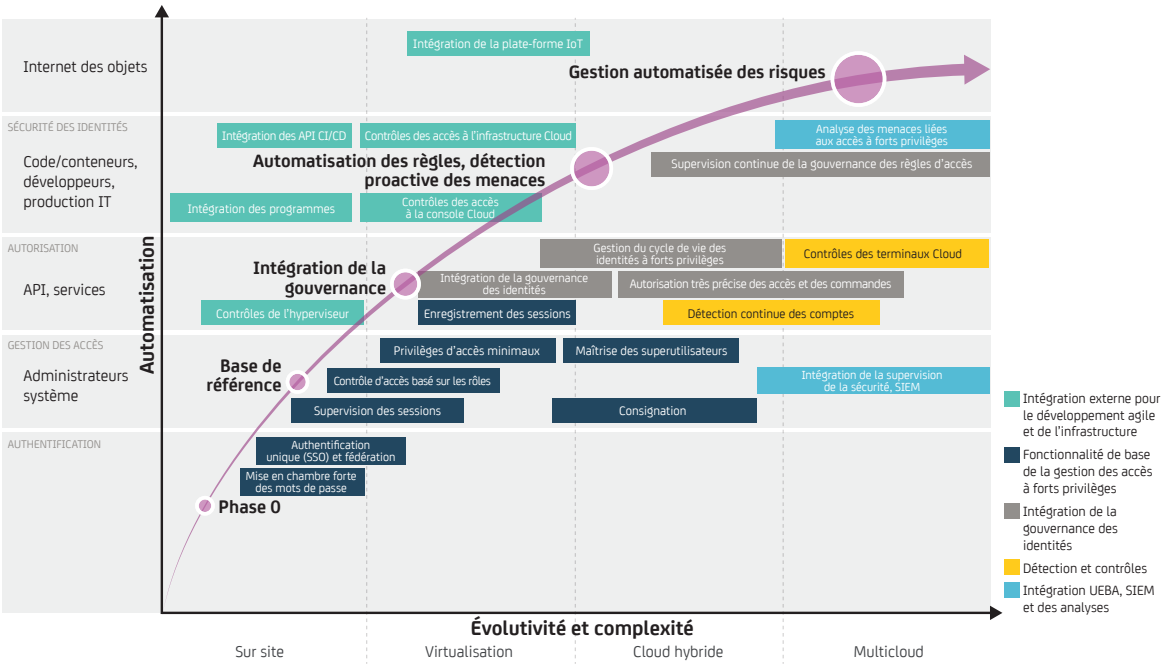
La transformation numérique accentue le défi de la gestion du risque lié aux accès à forts privilèges

Inévitablement, la transformation numérique modifie, accélère et automatise les interactions entre codes, machines et identités humaines. Les inquiétudes en termes de risque et de sécurité sont amplifiées en raison des initiatives de transformation numérique qui entraînent inéluctablement une augmentation du nombre de points d'accès à l'infrastructure de l'entreprise qui sont situés en dehors des contrôles existants et sont accessibles par des identités plus nombreuses et plus variées qu'auparavant, et qui prolifèrent à l'intérieur d'une infrastructure distribuée et dynamique (sur site, virtuelle et Cloud).

Pour permettre l'automatisation, la vitesse et l'évolutivité, il est crucial de déterminer quelles identités doivent avoir accès à des ressources et à des services particuliers, de gérer leurs informations d'identification en fonction des ressources et de garantir que l'accès est approprié.

De plus, pour s'adapter à la révolution de la mobilité, les entreprises doivent se préparer à l'Internet des objets (IoT) qui augmente significativement le volume des transactions dans leur infrastructure. En raison de l'adoption des outils de transformation numérique, le « qui » de l'équation de la gestion des accès change considérablement, et ce même avant d'y ajouter le « quoi » avec les équipements IoT.

Pour que la gestion des accès à forts privilèges facilite la transformation numérique au lieu de générer un goulet d'étranglement, la technologie et les outils doivent fournir une solution extensible et consolidée contre les risques générés par cette transformation.



Gouvernance intégrée

Les approches manuelles reposant sur un processus de certification humain ne peuvent pas se mettre à l'échelle de l'entreprise lorsque la transformation numérique accroît à la fois le nombre d'utilisateurs disposant d'un accès à forts privilèges en dehors des rôles d'administrateur système traditionnels et le nombre d'entités pouvant agir en tant qu'identités à forts privilèges. Pour trouver un équilibre entre agilité et sécurité dans ces nouveaux scénarios d'accès, les demandes d'autorisation et de rôle doivent être gérées via un processus de gouvernance intégré, que ces scénarios concernent des développeurs disposant d'un accès à des informations d'identification à forts privilèges en production, des conteneurs virtualisés et des hôtes dotés d'autorisations pour des sources de données ou des administrateurs avec des accès superutilisateur aux services Cloud.

Automatisation des règles

Les architectures de développement et de déploiement Cloud hybrides qui s'étendent sur des ressources sur site, des data centers virtualisés et des environnements Cloud publics peuvent donner lieu à une approche fragmentée et cloisonnée des identités à forts privilèges. Pour assurer une certaine cohérence (et éviter l'obligation d'un fournisseur unique), des règles de gouvernance et de contrôle des accès centralisées doivent être appliquées de façon dynamique aux comptes à forts privilèges propres à l'environnement (comme des comptes superadministrateurs AWS).

Détection proactive des menaces

Contrairement à la gestion des accès avec mot de passe partagé pour une infrastructure statique (comme un serveur de data center physique), les entreprises doivent désormais gérer l'autorisation, la supervision et la consignation des accès à des informations d'identification à forts privilèges pour un jour, une heure, voire quelques minutes, même si les changements apportés ou les actions réalisées avec ces identifiants sont légitimes et n'accroissent pas le risque. Le choix d'une approche « en contexte » tirant parti de l'apprentissage machine et de l'analyse comportementale peut favoriser la détection en temps réel et déclencher les mesures d'atténuation de risque même dans des environnements dynamiques et éphémères.

Gestion automatisée du risque

L'adoption de l'IoT introduit non seulement un nouveau type d'identité à forts privilèges machine sous la forme de contrôleurs d'équipement IoT, mais le recours à cette technologie contribue aussi à une augmentation potentiellement exponentielle des transactions devant être explicitement autorisées et supervisées pour se prémunir d'attaques éventuelles. Pour faire face à la multiplication des identités et au volume des transactions effectuées par des identités à forts privilèges, il est nécessaire de recourir à un modèle automatisé efficace en matière de détection des menaces et prenant en charge les mécanismes permettant d'évaluer le risque et d'implémenter leur atténuation, sans trop perturber les processus métier.

Section 3

Gouvernance intégrée et automatisation des règles : une étape à la fois

La gestion et la sécurisation des accès à forts privilèges dans un contexte de transformation numérique est un défi urgent, mais pas insurmontable.

Toutefois, étant donné que les informations d'identification des utilisateurs à forts privilèges sont de plus en plus utilisées (avec succès) pour obtenir un accès non autorisé, il est nécessaire de suivre un modèle de maturité pour limiter les angles morts au niveau des règles et de la supervision, et permettre un modèle de détection proactif via des analyses basées sur l'apprentissage machine qui renforcent la valeur des investissements existants et améliorent la précision.

Pour faciliter la transformation numérique plutôt que lui nuire, l'accès à forts privilèges à l'infrastructure, aux systèmes sensibles et aux données doit être basé sur un ensemble de phases réalistes et coordonnées dans le contexte d'un modèle de maturité. L'action la plus évidente consiste à réduire le nombre d'étapes manuelles nécessaires pour fournir l'accès à des informations d'identification à forts privilèges et à lier les décisions d'autorisation à des règles clairement définies.

Par ailleurs, plus la gestion des accès à forts privilèges est étroitement intégrée aux processus de gestion du cycle de vie des identités, plus les équipes de sécurité peuvent permettre l'automatisation à l'échelle de l'entreprise. L'application de contrôles automatisés aux rôles et aux autorisations d'accès affectés aux identités à forts privilèges peut aider de façon proactive à détecter des violations, comme le fait qu'un développeur ait reçu l'accès à des informations d'identification du code en production.

Il est essentiel que les outils de gestion des accès à forts privilèges soient en mesure de prendre en charge eux-mêmes l'automatisation durant le processus d'autorisation. Il est aussi important qu'ils facilitent l'évolutivité grâce à la prise en charge des opérations dynamiques et de l'infrastructure éphémère, comme les comptes d'administration AWS pour les identités humaines.

Beaucoup d'approches existantes sur la gestion des accès à forts privilèges sont fondées sur la couverture d'un sous-ensemble d'identités à forts privilèges et n'ont pas été conçues spécifiquement pour une infrastructure IT moderne. Afin d'avancer dans les phases d'un modèle de maturité, les entreprises doivent tenir compte de la façon dont les approches de gestion des accès à forts privilèges répondent à la prolifération, à la distribution et à la transformation des identités à forts privilèges. Ces approches doivent remplir les objectifs suivants :

- Étendre la gouvernance et la visibilité des identités à forts privilèges depuis l'infrastructure sur site jusqu'aux data centers virtualisés et aux services Cloud
- Automatiser l'autorisation des accès à forts privilèges sur la base d'exigences opérationnelles grâce à l'intégration de règles basées sur les rôles en matière de gestion des identités, plutôt que recourir à des processus d'approbation manuels
- Mettre les contrôles et la supervision à l'échelle de l'entreprise et les intégrer à une infrastructure dynamique et éphémère
- Faciliter la gouvernance et la supervision continues centralisées pour identifier le moment où des privilèges excessifs sont initialement accordés et déclencher un workflow de mesures correctrices
- Permettre la détection et la remédiation à mesure de l'évolution des nouvelles menaces grâce à l'apprentissage machine et à des modèles fondés sur les données

Section 4

Le risque et son contexte

Étant donné que les programmes de transformation numérique aboutissent à des réseaux distribués, à des taux de changement élevés, ainsi qu'à des volumes de transactions et d'identités à forts privilèges plus importants, ils soulèvent un défi pour les approches traditionnelles basées sur des règles : ces approches, qui se sont déjà révélées inappropriées, même pour les menaces existantes, peuvent difficilement détecter l'utilisation abusive ou le vol d'informations d'identification à forts privilèges.

Le choix d'une approche généralisée pour analyser les accès à forts privilèges et transmettre davantage de données dans les systèmes de gestion des événements et des informations de sécurité (Security Information and Event Management, SIEM) passe à côté du contexte important permettant aux analystes de sécurité et à la production IT de faire la distinction cruciale entre une incohérence, une anomalie majeure et une activité à risque élevé nécessitant une action correctrice immédiate.

À la place, il s'avère nécessaire de recourir à une approche propre au domaine, exploitant le contexte et les connaissances sur les rôles des utilisateurs à forts privilèges ainsi que leurs comportements, en vue d'affiner les recherches et de retrouver les actions représentant une preuve concrète d'une attaque ou d'une mise en danger.

Ce type d'approche fonctionne sur les mêmes principes que la définition des bases de référence du comportement. Elle prend en compte les actions prises par les utilisateurs à forts privilèges, ce qu'ils ont fait par le passé et le niveau ou risque associé à ces actions, y compris la sensibilité de la ressource cible et leur méthode d'accès aux systèmes. Néanmoins, cette approche doit également inclure un graphique des relations entre entités replaçant le comportement dans son contexte.

Section 5

Connaître vos utilisateurs à forts privilèges, c'est connaître vos risques

Une meilleure identification des attaques exploitant des informations d'identification n'est pas qu'une question d'accumulation de données. Il s'agit d'intégrer des données plus pertinentes sur le comportement des utilisateurs à forts privilèges, car celles-ci permettent d'identifier les modifications importantes représentant un véritable risque.

Cette approche est renforcée via l'intégration de systèmes de gouvernance des accès à forts privilèges pour permettre d'analyser le comportement des utilisateurs ayant des rôles similaires. Lorsqu'une machine ou un utilisateur à forts privilèges accède à un système incohérent avec son rôle et ses homologues, ou bien qu'il accède à un système à partir d'une adresse IP différente de l'adresse IP habituelle et qu'il effectue des tâches incohérentes par rapport aux schémas passés, le système peut détecter de manière plus précise un comportement ressemblant à celui d'une attaque afin d'activer l'action correctrice appropriée.

Section 6

Conclusion

La transformation numérique ne se fait pas en un jour, mais elle passera inévitablement par l'automatisation de l'application de règles de sécurité pour les identités les plus à risque et de la détection des éventuelles menaces provenant d'une utilisation inappropriée de ces identités à forts privilèges. En implémentant une approche basée sur les risques, vous avez la garantie que les analyses et contrôles de sécurité peuvent fonctionner en parallèle avec le programme de transformation numérique et permettre l'automatisation, la mise à l'échelle et la vitesse, sans compromis et de manière rentable. Cette transformation nécessite une feuille de route bien préparée qui s'étend sur plusieurs années, anticipant les exigences sur le court terme et le long terme, comme une solution de gestion des accès à forts privilèges, et assurant l'évolutivité et l'étendue requises à un coût raisonnable de propriété, tout au long du cycle de vie.

La sécurité est impérative, mais son étendue, son évolutivité et son coût ne peuvent pas constituer un obstacle à la transformation numérique.

Pour plus d'informations sur les avantages que CA PAM peut apporter à votre entreprise, rendez-vous sur le site **ca.com/pam**.

ca technologies

Restez connecté à CA Technologies sur ca.com/fr

CA Technologies (NASDAQ : CA) fournit les logiciels qui aident les entreprises à opérer leur transformation numérique. Dans tous les secteurs, les modèles économiques des entreprises sont redéfinis par les applications. Partout, une application sert d'interface entre une entreprise et un utilisateur. CA Technologies aide ces entreprises à saisir les opportunités créées par cette révolution numérique et à naviguer dans « l'Économie des applications ». Grâce à ses logiciels pour planifier, développer, gérer les performances et la sécurité des applications, CA Technologies aide ainsi ces entreprises à devenir plus productives, à offrir une meilleure qualité d'expérience à leurs utilisateurs et leur ouvre de nouveaux relais de croissance et de compétitivité sur tous les environnements : mobile, Cloud, distribué ou mainframe. Pour plus d'informations, rendez-vous sur le site **ca.com/fr**.

CS200-270334_0517