LIVRE BLANC | JUIN 2017

Gestion des accès à forts privilèges : feuille de route pour le calcul du coût total de possession

Découvrez les coûts cachés et les avantages de votre approche d'implémentation PAM

ca technologies

Table des matières

Section 1

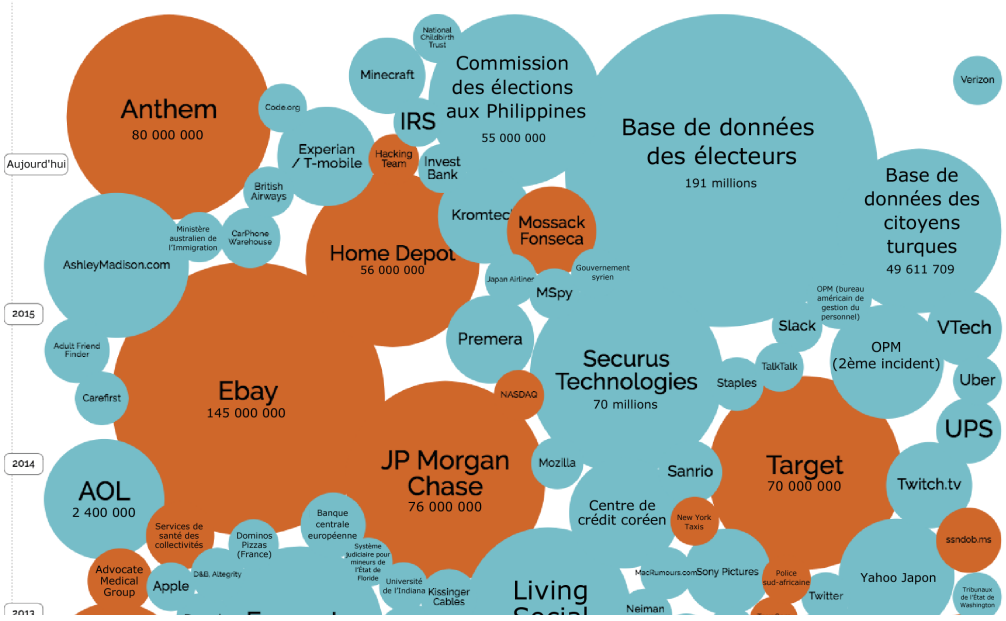
Introduction

Qu'ils soient usurpés, exploités de manière abusive ou mal utilisés accidentellement, les comptes d'utilisateurs à forts privilèges se trouvent au cœur de la plupart des violations de données. Les équipes de sécurité évaluent de plus en plus les solutions complètes de gestion des accès à forts privilèges (Privileged Access Management, PAM) pour éviter les dommages susceptibles d'être causés par un utilisateur non autorisé ayant obtenu des privilèges élevés ou par un utilisateur à forts privilèges pouvant être fatigué, stressé ou commettant tout simplement une erreur. La pression exercée par les dirigeants et les équipes d'audit en vue d'une réduction de l'exposition des activités incite ces équipes à renforcer leurs efforts, mais, selon la stratégie d'implémentation adoptée, les solutions PAM complètes peuvent entraîner des coûts cachés. En raison de ses différentes fonctionnalités (chambres fortes de mots de passe, gestion et supervision des sessions, et souvent aussi analyses du comportement utilisateur et renseignements sur les menaces), une solution de gestion des accès à forts privilèges peut exercer un impact majeur sur le coût et les avantages qu'elle offre en fonction de la façon dont elle est implémentée. Le présent rapport fournit un schéma directeur permettant de déterminer les coûts directs, indirects et cachés du déploiement d'une telle solution au fil du temps.

Section 2

Comptes à forts privilèges et violations de grande envergure

Les violations de sécurité de grande envergure sont devenues une constante dans l'actualité du secteur. Selon les experts, 80 à 100 % d'entre elles impliquent l'utilisation de comptes à forts privilèges. De plus en plus d'attaques exploitent des comptes d'administrateurs IT, de développeurs d'applications, de responsables métier, de partenaires, de fournisseurs et de cadres dirigeants. Une fois que l'auteur se trouve à l'intérieur du système, il peut se déplacer de manière horizontale et verticale pour accéder à des informations sensibles et installer des programmes malveillants sources de dommages futurs. Il est toutefois difficile pour un administrateur IT de déterminer si l'accès d'un utilisateur à forts privilèges à des zones sensibles est problématique ou non, puisqu'il peut s'agir d'une activité quotidienne normale.



En clair, le rôle de l'utilisateur à forts privilèges peut être le maillon faible de la chaîne de sécurité d'une organisation, quelle que soit sa taille, partout dans le monde. Prendre correctement en main ce problème pourrait dès lors s'avérer très rentable dans les années à venir.

Section 3

Se protéger contre les violations des comptes à forts privilèges grâce à l'approche PAM

La sécurité des informations recouvre de nombreux aspects ; la gestion des accès à forts privilèges n'est que l'un d'entre eux. En général, les organisations commencent à se pencher sérieusement sur la gestion des accès à forts privilèges pour l'un des deux motifs suivants :

- Elles rencontrent un grave problème (par exemple, elles ont subi une violation ou n'ont pas rempli les exigences de conformité).
- Elles sont prêtes à implémenter les meilleures pratiques.

Quelle qu'en soit la raison, il n'est pas rare d'émettre des hypothèses sur l'implémentation d'une solution de gestion des accès à forts privilèges. Il peut être tentant d'avoir une vision à court terme, en partant du principe qu'il est possible de commencer par un ensemble de fonctionnalités limité, puis d'augmenter le périmètre et l'échelle de l'implémentation au fil du temps. Bien que cette stratégie puisse être acceptable si elle est accompagnée d'autres mesures de sécurité, l'expérience montre qu'en ce qui concerne la gestion des accès à forts privilèges, elle n'est pas très réaliste, tant du point de vue financier que technique. En réalité, il s'agit d'un domaine où il est extrêmement important d'adopter une vision à long terme : il faut non seulement protéger les périphériques, les terminaux, les utilisateurs et les comptes, mais il faut aussi tenir compte des problèmes de mise en conformité ainsi que de la feuille de route de l'entreprise. Tous ces éléments auront des répercussions sur le coût total de possession.

Périphériques

Aujourd'hui, il ne suffit plus de protéger les terminaux traditionnels. Le périmètre s'est élargi aux environnements virtualisés, aux conteneurs et aux systèmes Cloud. Les infrastructures IT hybrides, les consoles de gestion, les nombreuses ressources et les changements constants peuvent étendre la surface d'attaque disponible. Pour assurer une protection appropriée, il faut mettre en place des mesures intégrant l'ensemble de votre environnement dès le début, pour que vous puissiez garantir une protection d'envergure et en profondeur, adaptée aux menaces. Vous devez prendre en compte ce type de besoins futurs lorsque vous planifiez une implémentation de gestion des accès à forts privilèges.

Utilisateurs

Le hameçonnage et l'ingénierie sociale sont désormais des méthodes courantes pour obtenir des informations d'identification des utilisateurs à forts privilèges. Les menaces externes (mais aussi de plus en plus les menaces internes) exigent des informations contextuelles complètes : nous devons d'abord comprendre le comportement normal d'un utilisateur à forts privilèges avant de pouvoir isoler les comportements anormaux. Le concept même d'un utilisateur à forts privilèges évolue avec l'adoption des méthodes de développement agile, hybride et Cloud : par exemple, les responsables métier peuvent recevoir des privilèges d'administration pour les solutions CRM Cloud. Pour compliquer la situation, le comportement de l'utilisateur change au fil du temps et les attaques ciblées se transforment. Il devient donc difficile d'assurer avec certitude si un compte a été compromis. Les solutions de gestion des utilisateurs à forts privilèges doivent apprendre et s'améliorer en continu pour pouvoir identifier les violations possibles.

Conformité

Exigence constante pour les organisations de toutes les tailles, le respect de la conformité (et le fait de savoir le prouver) peut rapidement mener à une « fatigue réglementaire » en raison du volume et de la portée des changements de réglementation.

Les technologies PAM doivent prendre en charge les réglementations régissant les contrôles et les processus utilisés pour assurer la cybersécurité. Cela peut inclure la documentation de l'accès aux paramètres de configuration et aux données privées, le respect d'ITIL® et la fourniture de pistes d'audit définitives pour l'HIPAA (Health Insurance Portability and Accountability Act) de 1996, la norme PCI DSS (Payment Card Industry Data Security Standard) et d'autres réglementations. La preuve de la conformité doit être pensée dès le départ ; elle ne doit pas être une option de second plan.

Section 4

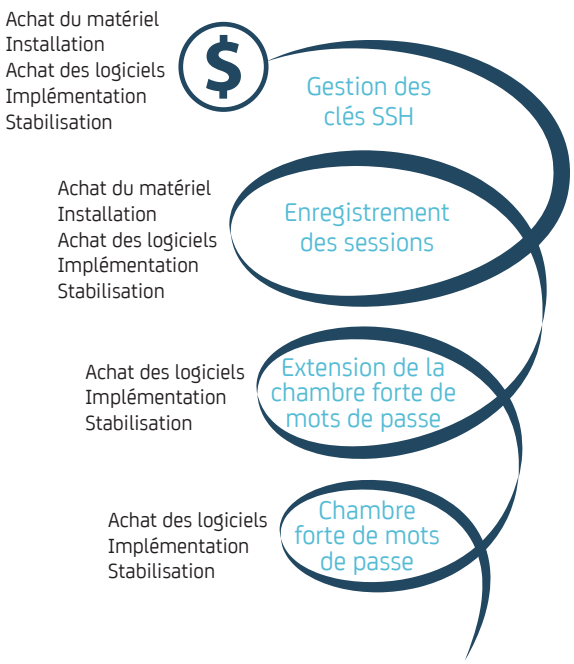
La stratégie d'implémentation PAM exerce un impact majeur sur le coût total de possession

La méthode d'implémentation choisie pour une solution PAM a des conséquences majeures sur le coût total de possession. Il est important de comprendre les deux méthodes d'implémentation d'une solution de gestion des accès à forts privilèges.

La première méthode (que nous appellerons « la méthode complète ») consiste d'abord à créer une feuille de route des principales exigences, puis à fournir un produit doté de toutes les fonctionnalités nécessaires (y compris pour les exigences futures) dès le départ, pour ensuite développer l'échelle et le périmètre des fonctionnalités au fil du temps, étape par étape. Par exemple, si vous avez besoin des fonctionnalités de mise en chambre forte de mots de passe, d'enregistrement des sessions et de gestion des clés Secure Shell (SSH), vous pouvez acquérir un produit incluant l'ensemble de ces fonctionnalités et les activer lorsque cela est nécessaire. Comme toutes ces fonctionnalités sont intégrées, il ne sera pas nécessaire de prévoir une longue période de stabilisation.

La deuxième méthode (que nous appellerons « la méthode morcelée ») commence aussi par l'établissement d'une feuille de route, mais les produits sont mis à disposition au fil des besoins. Par exemple, en prenant une feuille de route incluant les trois mêmes fonctionnalités que celles citées auparavant, vous pouvez commencer par l'achat de la chambre forte de mots de passe, puis, au bout de quelques mois, une fois son implémentation et sa stabilisation terminées, vous pouvez vous rapprocher du fournisseur pour acquérir la fonctionnalité d'enregistrement des sessions (et tout le matériel supplémentaire nécessaire), l'implémenter et la stabiliser sur six mois, et, enfin, en faire de même avec la fonctionnalité de gestion des clés SSH.

La méthode choisie peut affecter aussi bien le coût total de possession que le délai de rentabilisation. L'implémentation d'une solution de gestion des accès à forts privilèges complète, intégrée et bâtie sur des fonctionnalités de collecte d'informations peut offrir à la fois un délai de rentabilisation plus rapide et un coût total de possession (TCO) inférieur. Les coûts sont connus et prévisibles. En revanche, lorsque l'implémentation est morcelée, le déploiement initial peut être simple : une chambre forte de mots de passe qui, dans un premier temps, ne contient que quelques comptes, mais qui grossira progressivement, puis, ultérieurement, l'ajout de l'enregistrement des sessions. Toutefois, les coûts deviennent imprévisibles, car ceux liés à l'infrastructure peuvent varier à chaque module ajouté. Par ailleurs, le client est « enfermé » chez un seul fournisseur, qui n'est peut-être pas le fournisseur idéal pour lui. Les calculs du coût total de possession doivent prendre en compte le coût, le temps et l'exposition liés à l'ajout de l'échelle et du périmètre dans une implémentation morcelée. Les coûts incluent à la fois les coûts matériels (coût des licences, infrastructure et autres) et immatériels (délai de rentabilisation, exposition prolongée au risque, coûts d'intégration et de maintenance, etc.). La génération de scripts et la maintenance liées à l'ajout de terminaux supplémentaires pour la mise en chambre forte de mots de passe peut, par exemple, être très différente de ce qui est nécessaire pour la gestion des clés SSH.



Pour avoir une meilleure idée des questions à poser et des fonctionnalités à évaluer, il peut être utile de comprendre de quoi se compose une solution PAM complète et de savoir déterminer les avantages qualitatifs et quantitatifs vis-à-vis du coût financier qu'elle engendre.

Section 5

Principaux composants d'une solution de gestion des accès à forts privilèges complète

Une solution de gestion des accès à forts privilèges complète se compose de plusieurs éléments clés, comme la capacité à contrôler les accès à forts privilèges sur l'ensemble des ressources, à sécuriser le stockage des informations d'identification à forts privilèges, à superviser et à enregistrer l'activité, à protéger les consoles Cloud hybrides et les API de gestion, ainsi qu'à analyser le comportement de l'utilisateur en vue de détecter les anomalies susceptibles d'indiquer des mises en danger. Quelques informations à retenir lors de l'évaluation d'une solution PAM :

Chambre forte de mots de passe : une chambre forte (ou coffre-fort) de mots de passe chiffrée et renforcée pour le stockage des informations d'identification gère les mots de passe et d'autres identifiants ou jetons en les modifiant à des intervalles configurables, conformément aux règles définies. Cela permet de protéger les comptes d'administration, partagés et de service, ainsi que les comptes d'application à application et les environnements Cloud hybrides. Toutefois, la mise en chambre forte des mots de passe seule ne suffit pas.

Supervision des sessions : dans un premier déploiement morcelé, ce composant essentiel manque souvent dans la pratique. La capacité à initier automatiquement une session distante qui enregistre, analyse et supervise une session d'utilisateur à forts privilèges permet une supervision en temps réel et une analyse post-session. Cette fonctionnalité ne doit pas être ajoutée après coup : lorsqu'un utilisateur à forts privilèges viole une règle ou affiche un comportement anormal, vous voulez commencer la supervision immédiatement, pas six mois plus tard.

Environnements hybrides : une solution PAM complète peut contrôler l'accès à forts privilèges aux ressources Cloud, aux machines virtuelles et aux hyperviseurs, en plus de l'accès aux environnements de data center physique traditionnel. La détection automatique est essentielle puisque les nouvelles ressources peuvent être ajoutées à l'environnement en quelques minutes.

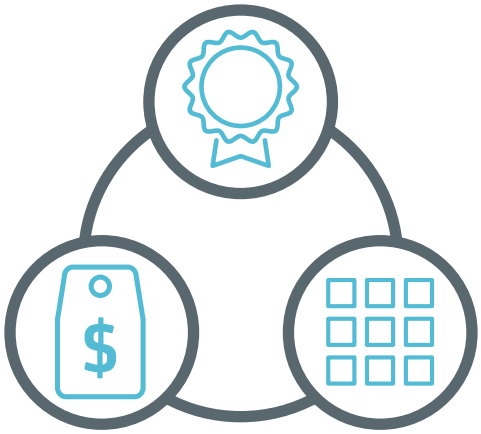
Analyse du comportement utilisateur : une solution PAM complète sait faire la différence entre un comportement de l'utilisateur à forts privilèges normal et un comportement anormal afin de déclencher des mécanismes de protection supplémentaires en cas d'anomalies. Elle collecte des données contextuelles propres au domaine et effectue des analyses avancées pour créer des modèles de risque basés sur les schémas de comportement précédents. Lorsqu'elle détecte un comportement inhabituel, elle peut déclencher automatiquement une authentification supplémentaire (Radius, TACACS+ ou CA Advanced Authentication) ou un enregistrement des sessions.

Une solution PAM complète, en plus d'offrir ces fonctionnalités, permet une implémentation et une livraison rapides des fonctionnalités de détection et des informations prêtes à l'emploi. Par ailleurs, elle nécessite peu de compétences spécialisées pour bénéficier d'avantages immédiats. Elle doit permettre aux administrateurs d'examiner facilement les incidents et de comprendre l'utilisation de leurs comptes à forts privilèges.

Section 6

Évaluation de l'impact métier d'une solution PAM complète pour l'organisation

Quels sont les éléments qui rentrent en jeu dans la détermination du coût et des avantages, compte tenu des exigences susmentionnées ? À un haut niveau, il convient d'évaluer trois types d'éléments : le coût financier, les avantages qualitatifs et les avantages quantitatifs. Basés sur les moyennes du secteur et les pratiques propres à une organisation, les avantages quantitatifs sont relativement aisés à déterminer. Quant aux avantages qualitatifs, ils sont un peu plus difficiles à mesurer, mais des éléments comme le délai de détection ou la facilité d'utilisation peuvent avoir un impact significatif. Nous allons vous aider à aborder chacun de ces aspects dans les sections suivantes.



Éléments permettant de calculer les coûts financiers

Le calcul des coûts financiers est, en règle générale, un exercice assez simple, qui tient compte des éléments suivants :

- Les coûts d'acquisition de licence du produit (à usage unique, abonnement)
- Les coûts de maintenance du produit (deuxième phase et au-delà ; coût de support interne)
- Les coûts de déploiement du produit (services professionnels, déploiement, configuration)
- Les coûts de formation (formation client interne, formation utilisateur final)

Plusieurs points doivent être pris en compte dans le calcul des coûts financiers. Tout d'abord, il faut comparer le coût de l'implémentation d'une solution complète par rapport au coût de l'implémentation d'une solution morcelée. Avec une solution complète, le coût initial (qui comprend l'acquisition des licences, le déploiement et la formation) et les coûts de maintenance ultérieure entreront en jeu. Toutefois, avec une implémentation morcelée, le calcul doit aussi inclure le coût d'intégration, qui peut être directement proportionnel au nombre et à la taille des systèmes à intégrer. Si vous devez acquérir une solution PAM par étapes, plutôt que de manière globale, il faudra tenir compte des coûts d'acquisition, de formation et de déploiement incrémentiels en plus des coûts de base susmentionnés. Les coûts liés aux charges d'exploitation (OPEX) peuvent aussi être inclus à la décision de choisir une implémentation morcelée : les fonctionnalités supplémentaires nécessitent souvent un matériel dédié, qui devra être budgété, provisionné, configuré et mis à jour. Le calcul des coûts doit également prendre en compte les ressources, le temps et les compétences nécessaires à une approche morcelée, qui, avec autant d'inconnues, représente un véritable défi au processus de budgétisation.

Éléments à prendre en compte pour la détermination des avantages financiers qualitatifs

Il est parfois difficile d'évaluer les avantages financiers qualitatifs d'une telle solution, mais ils jouent un rôle majeur dans le choix entre une solution complète et une solution morcelée. Tout d'abord, nous allons étudier l'implémentation morcelée : commencez par une chambre forte de mots de passe pour quelques comptes, ajoutez-y des comptes à forts privilèges au fil du temps, intégrez-y l'enregistrement des sessions à une date ultérieure, puis, enfin, pensez à y intégrer les analyses du comportement utilisateur une fois le système en place.

Avantages :

- Il peut y avoir une réduction des coûts en amont.

Inconvénients :

- Le délai de rentabilisation est beaucoup plus long : il est impossible d'avoir de la visibilité assez rapidement pour atténuer efficacement les risques.
- Le risque est fortement augmenté en cas de violation : des fonctionnalités comme l'enregistrement des sessions demanderont des semaines ou des mois d'attente avant d'obtenir le matériel requis.
- La surface d'exposition au risque est augmentée pendant de longues périodes.
- Il peut être nécessaire de rédiger du code ou des scripts pour mettre l'implémentation à l'échelle.
- Des coûts supplémentaires sont nécessaires pour le matériel, la sauvegarde et la redondance : les coûts à plus long terme sont susceptibles d'être plus élevés.
- Vous êtes dépendant d'un fournisseur unique : chaque fois que vous envisagez un nouveau module, le processus d'approvisionnement repart de zéro ; il est possible que le calendrier des modules implémentés préalablement soit réinitialisé, ce qui implique un engagement plus long vis-à-vis du produit par rapport à ce qui a été planifié à l'origine.

Une solution intégrée et complète pouvant être implémentée d'un seul coup, quant à elle, implique de sélectionner une solution dotée de toutes les fonctionnalités nécessaires dès le début. Bien qu'il soit possible d'activer les fonctionnalités quand les besoins se font sentir, tout est prêt lorsque vous l'êtes. Ce type d'implémentation, notamment lorsqu'elle est livrée sous la forme d'une appliance, offre une atténuation du risque prête à l'emploi et ne nécessite aucune compétence spécifique pour générer des avantages immédiats. Cela réduit la charge de travail tout en évitant les violations.

Avantages :

- Déploiement et délai de rentabilisation rapides.
- Protection immédiate en cas de soupçon d'une violation : si l'enregistrement des sessions est nécessaire, il suffit de l'activer.
- Disponibilité immédiate de fonctionnalités supplémentaires comme les analyses pour assurer le contrôle et la visibilité de l'environnement.
- Surface d'attaque grandement réduite.
- Coût total inférieur : nul besoin de codage ni de création de scripts personnalisés ni de matériel supplémentaire.

Inconvénients :

- Les coûts en amont peuvent être supérieurs.

Certains facteurs technologiques peuvent aussi contribuer aux avantages financiers qualitatifs. Si la solution de gestion des accès à forts privilèges exploite les analyses du comportement utilisateur et l'intégration étroite avec les renseignements sur les menaces, la capacité à détecter une activité anormale et à prendre des mesures immédiates est fortement renforcée. Si la mise en cluster multisite est une fonctionnalité, cela peut mener à une hausse de la disponibilité et à un temps de réponse plus rapide. Si la solution est livrée sous la forme d'une appliance virtuelle ou physique, le délai d'implémentation sera beaucoup plus court que pour une solution logicielle. Enfin, il est important de tenir compte des coûts de maintenance qui peuvent être grandement inférieurs pour une appliance que pour une suite de produits logiciels nécessitant chacun son propre matériel dédié.

Le résultat, c'est que tous les éléments qualitatifs susmentionnés peuvent contribuer à un coût total de possession réduit, ainsi qu'à un délai de rentabilisation plus rapide.

Éléments à prendre en compte pour la détermination des avantages financiers quantitatifs

Concernant les avantages financiers quantitatifs, prenez en compte trois éléments clés : la réduction des coûts, les améliorations de la productivité et la protection du chiffre d'affaires.

Réduction des coûts

La réduction des coûts inclut l'évitement des coûts d'infrastructure, des coûts associés aux violations, des frais d'audit et de mise en conformité ainsi que des coûts liés aux interruptions de service non planifiées. Un autre élément à ne pas sous-estimer est la réduction des coûts de déploiement, de maintenance et de support.

Les coûts de l'infrastructure peuvent être évités en choisissant une solution PAM complète basée sur une appliance, contrairement à une solution logicielle ou morcelée. Cela est calculé en estimant le nombre de serveurs/appliances requis pour les solutions PAM existantes ou concurrentes, le coût par serveur, le nombre d'équilibreurs de charge requis et le coût pour chacun, ainsi que le pourcentage des coûts d'infrastructure qui pourraient être évités avec une solution basée sur une appliance.

Les coûts liés aux violations incluent les répercussions sur le chiffre d'affaires, les coûts de notification au client, les coûts de relations publiques et de réponse aux incidents ainsi que les frais juridiques. Le calcul de ces coûts nécessite une estimation de la probabilité d'une violation (l'estimation actuelle est de 22 % sur 2 ans), le volume d'enregistrements potentiellement exposés et le coût par enregistrement ainsi que le coût de remédiation et le pourcentage de ces coûts qui pourrait être évité grâce à une solution PAM complète. Étant donné que selon les estimations, la compromission des informations d'identification est à l'origine de plus de 80 % des violations, cet avantage peut être important.

Une gestion des accès à forts privilèges complète permet aussi de diminuer les coûts d'audit et de mise en conformité externes. Pour en calculer la réduction potentielle, estimez le nombre de problèmes de mise en conformité par année, le coût annuel des violations de la conformité, les coûts d'audit externe pour remédier à un problème pouvant faire l'objet d'un rapport et le pourcentage des frais d'audit, des actions correctrices et des pénalités pour non-conformité qui pourraient être évités grâce à l'utilisation d'une gestion des accès à forts privilèges complète.

Autre avantage financier : la probabilité d'avoir moins d'interruptions du système imprévues, qui peuvent nuire à la productivité et au moral des employés, en plus d'entraîner la perte de clients. Ce calcul inclut une estimation du nombre d'éventuelles interruptions d'activité par année dues à des violations de comptes d'utilisateurs à forts privilèges, ainsi que le temps d'indisponibilité moyen par interruption du système, le coût par minute et l'impact d'une hausse de la disponibilité.

L'un des principaux problèmes dans l'implémentation d'une solution PAM de façon morcelée est que le coût de déploiement et de maintenance augmente considérablement avec l'achat, l'implémentation et la stabilisation de chaque module. Des compétences spécifiques en matière de rédaction de scripts sont nécessaires, pourtant combien de clients voudront bien embaucher une personne à plein temps pour gérer, maintenir et déployer la solution ? L'achat d'une solution complète pour, par la suite, implémenter des fonctionnalités à mesure que le besoin s'en fait sentir évite ce coût.

Amélioration de la productivité

Les hausses de productivité prennent deux formes différentes : la réduction des coûts de main-d'œuvre des administrateurs système IT et la diminution des coûts d'implémentation et d'exploitation des applications.

Une solution PAM complète implique une diminution du temps que les administrateurs système consacrent à la détection, à l'application des règles, à la récupération ou à la regénération de mots de passe. Cette réduction de la charge de travail permet donc une hausse du temps disponible pour implémenter des solutions novatrices qui feront avancer votre activité. Pour calculer les réductions des coûts de main d'œuvre des administrateurs système IT, tenez compte du nombre de ressources et d'appareils ayant des informations d'identification d'accès à forts privilèges et du nombre de comptes par ressource/appareil/application. Déterminez ensuite le nombre de minutes requises par un administrateur IT pour fournir ou mettre à jour un accès à forts privilèges et le coût moyen par heure ainsi que la réduction de temps prévue pour mettre à jour les informations d'identification d'accès à forts privilèges grâce à l'utilisation d'une solution PAM complète.

Les coûts d'implémentation et d'exploitation peuvent être considérablement réduits grâce à l'utilisation d'une solution PAM complète basée sur une appliance. Pour calculer ces économies, considérez le nombre d'administrateurs système IT requis pour l'implémentation, l'hébergement et la gestion d'une solution existante ou concurrente ainsi que le coût moyen par heure et par année, puis appliquez le pourcentage de réduction des coûts à espérer lorsque vous opterez pour une solution PAM complète basée sur une appliance.

Protection du chiffre d'affaires

Une gestion PAM complète contribue grandement à atténuer les plus graves conséquences financières d'une violation de données. Pour calculer cet avantage financier, estimez l'impact qu'une atteinte à votre image de marque aurait sur le chiffre d'affaires suite à une violation du système ou des données, et estimez aussi le pourcentage de protection du chiffre d'affaires grâce à une réduction du risque de compromission des informations d'identification. Un récent rapport du Ponemon Institute montre que pour les entreprises américaines interrogées en 2016, l'impact financier sur le chiffre d'affaires suite à une atteinte à leur image de marque et à la perte de clientèle s'élevait à 3,97 millions de dollars par an. La gestion des accès à forts privilèges peut donc avoir un impact financier important.

Section 7

Unifier

Le besoin d'une solution de gestion des accès à forts privilèges complète se fait clairement sentir. La méthode de calcul du coût total de possession comprend divers éléments à prendre en considération. Les coûts dépendent du choix entre l'implémentation d'une solution PAM complète, permettant d'activer les fonctionnalités au fil des besoins, ou l'implémentation morcelée avec prise en compte des coûts ultérieurs. Retenez les coûts et les avantages qu'offre une approche complète :

- Les coûts sont prévisibles et faciles à budgéter ; il n'y a pas à prévoir les coûts supplémentaires associés à une approche morcelée (approvisionnement, licences, formation, déploiement, ressources et infrastructure supplémentaire).
- Les avantages qualitatifs sont importants : délai d'implémentation et de rentabilisation rapide, protection immédiate en cas de violation, surface d'attaque réduite et coût total de possession inférieur.
- Les avantages quantitatifs sont tout aussi impressionnants : vous évitez les coûts liés à l'infrastructure, vous diminuez les coûts liés aux violations ainsi que ceux associés aux audits et à la mise en conformité, vous évitez les interruptions de service non planifiées et vous réduisez les coûts de déploiement, de maintenance et de support.

Bien évidemment, les résultats de ces calculs varient selon la situation et les préférences de l'organisation, mais il est évident qu'une approche par implémentation complète aboutit à un coût total de possession beaucoup plus favorable qu'une approche morcelée pour implémenter une gestion des accès à forts privilèges.

Section 8

Conclusion : une vision à long terme du coût total de possession

Les surfaces d'attaque non protégées grandissent de jour en jour, ce qui augmente le risque pour les organisations. Une solution de gestion des accès à forts privilèges complète permet de réduire ces surfaces tout en offrant un délai de rentabilisation extrêmement rapide, ce qui est très important lorsqu'une organisation court le danger de connaître une violation. Dès le premier jour, elle fournit toutes les fonctionnalités nécessaires. Si, à l'origine, vous préférez n'activer que certaines d'entre elles, toute la puissance de la solution est disponible en un instant en cas de soupçon de violation. Les calculs prouvent qu'une solution de gestion des accès à forts privilèges complète basée sur une appliance présente des avantages à long terme aussi bien au niveau financier qu'en termes de productivité et métier.

Pour plus d'informations sur les avantages que les solutions CA PAM peuvent apporter à votre organisation, 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**.

1 Thomson Reuters, « Cost of Compliance 2016 », https://risk.thomsonreuters.com/en/resources/special-report/cost-compliance-2016.html

2 Ponemon Institute, « 2016 Cost of Data Breach Study: Global Analysis », juin 2016, https://securityintelligence.com/media/2016-cost-data-breach-study/

3 Ibid.

CS200-282765_0617