Trois bonnes raisons pour une gestion de l'identité des comptes privilégiés (et un avantage étonnant)

Auteur du livre blanc : ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™)
Elaboré pour le compte de Centrify

février 2015

IT & DATA MANAGEMENT RESEARCH, INDUSTRY AND ANALYSIS & CONSULTING

Trois bonnes raisons pour une gestion de l'identité des comptes privilégiées (et un avantage étonnant)

Table des matières

Trois bonnes raisons pour une gestion de l'identité des comptes privilégiées (et un avantage étonnant)

Présentation générale

L'accès des comptes à privilèges est l'un des aspects les plus sensibles en informatique. Les comptes administrateurs ont la capacité de réaliser des changements radicaux et fondamentaux dans les systèmes informatiques dont dépendent les sociétés. Lorsqu'utilisés de manière frauduleuse, leur impact peut causer de vastes dégâts allant du non-respect des conformités donnant droit à des amendes, en passant par des incidents de sécurité causant une perte de confiance dans la marque et une perte de revenus.

Pour ces raisons et pour d'autres encore, la visibilité et le contrôle des accès privilégiés sont recommandés et sont souvent obligatoires :

- Par le biais d'un ensemble d'obligations règlementaires
- Pour garantir une gestion responsable de l'entreprise
- Pour améliorer la sécurité

La gestion des comptes à privilèges traite de ces problèmes et de ces questions et d'autres également. Dans ce rapport, les analystes d'ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) étudient les façons dont la visibilité et le contrôle des comptes à privilèges aident les entreprises à atteindre leurs objectifs mais fournissent également un avantage que beaucoup ne voient pas : une meilleure fiabilité de l'informatique susceptible de réduire les coûts d'exploitation. Cet étude examine les caractéristiques d'une solution efficace et fournit également la preuve que l'étude d'EMA soutient les valeurs d'une approche plus cohérente du contrôle opérationnel de l'informatique.

L'accès privilégié : ses avantages et ses risques

Quand il s'agit d'accéder et de manipuler des systèmes informatiques particulièrement précieux pour l'entreprise, les utilisateurs privilégiés tels que les administrateurs ont typiquement la plus large latitude opérationnelle qui soit. En général, les utilisateurs les plus chevronnés au sein d'un département informatique sont responsables du déploiement et de la gestion des fonctionnalités dont dépendent l'entreprise, allant des tâches quotidiennes essentielles aux fonctionnalités stratégiques qui permettent à l'entreprise de maintenir son avance sur sa concurrence. Ils peuvent également avoir une responsabilité considérable dans leur secteur d'activités comme la gestion des applications commerciales.

Mais ce pouvoir comporte des risques. La complexité de l'informatique est telle, que même les modifications effectuées par les salariés les plus chevronnés peuvent avoir des impacts inattendus et graves sur la disponibilité, l'exécution et/ou l'intégrité des ressources. Les personnes malveillantes, à l'intérieur de l'entreprise et en dehors, peuvent profiter de l'accès au niveau administrateur pour causer des sérieux dégâts dans les affaires d'une société. Etant donné la sophistication et la discrétion de plus en plus évoluées des attaques d'aujourd'hui réalisées par le biais de malware et autres méthodes, il est commun pour des pirates d'obtenir et d'exploiter de tels privilèges en usurpant l'identité d'un collaborateur digne de confiance.

Typiquement, les utilisateurs privilégiés tels que les administrateurs ont la latitude opérationnelle la plus large, mais ce pouvoir comporte des risques.

La Gestion des comptes à privilèges : Pas simplement une bonne idée …

Les entreprises cherchent de plus en plus à renforcer les contrôles des accès à privilèges pour les raisons suivantes.

Pour le respect de la conformité

Un certain nombre de mesures réglementaires recommandent ou rendent obligatoire le contrôle spécifique de la gestion des risques sur les accès des comptes à privilèges. La règlementation comme le « Sarbanes-Oxley Act » (« SOX »), par exemple, oblige les entreprises publiques à déployer des processus et des contrôles afin de garantir la gestion responsable de celles-ci.

Vu l'importance élevée de l'informatique dans la gestion et la documentation des entreprises ainsi que dans leur performance, protéger les systèmes d'informations des entreprises contre les abus des privilèges administrateurs est l'une des manières les plus concrètes pour garantir un contrôle efficace.

Trois bonnes raisons pour une gestion de l'identité des comptes privilégiées (et un avantage étonnant)

La « Payment Card Industry Data Security Standard (PCI DSS) version 3.0 » exige des mesures semblables pour protéger les données des détenteurs de cartes bancaires, en particulier dans le cadre de la séparation des fonctions (Code des bonnes pratiques et exigences n°6) mais également dans le cadre de la surveillance et de l'application du contrôle des accès à privilèges (obligations 7 et 8).

Dans le secteur public, le North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards, exige non seulement l'authentification, le contrôle des accès, la délégation d'accès et les séparations des pouvoirs mais exige également dans les faits le contrôle continu et intégral des accès, leur archivage et leur audit.

Au niveau du gouvernement, les conseils prodigués dans le « U.S. National Institutes of Standards and Technology (NIST) Special Publication 800-53A Rev 4 » sont largement cités ; dans la même ligne de conduite, il recommande le contrôle des accès informatiques critiques, la séparation des pouvoirs et un soin particulier concernant les accès administrateurs.

Les mesures du gouvernement impactent également des secteurs d'activité tels que la santé. Aux États-Unis, la loi sur la sécurité adoptée pour mettre en application les dispositions du Health Insurance Portability and Accountability Act (HIPAA) (loi sur la portabilité et la responsabilité en assurance santé) parle du contrôle des accès comme d'un élément spécifique pour sauvegarder les données médicales électroniques protégées.

Pourquoi ces mandats parlent-ils tellement du besoin systématique de contrôler et de surveiller les accès privilégiés ?

Pour garantir la confiance relatives aux bonnes pratiques commerciales

La plupart du temps, les accès privilégiés contrôlent les aspects les plus fondamentaux de l'informatique, du déploiement et à la configuration à l'état brut, en passant par les nuances de la gestion des applications et de l'expérience de l'utilisateur final. Sans contraintes, cette capacité peut s'avérer extrêmement endommagée, et pas seulement pour les systèmes informatiques sensibles d'une entreprise.

La loi « Sarbanes-Oxley Act » et la norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS), par exemple, met l'emphase sur la séparation des pouvoirs de façon à garantir un contrôle responsable des processus commerciaux. La gestion et la surveillance informatiques aident à garantir que les SI des entreprises ne soient l'objet de manœuvres frauduleuses pour pirater les entreprises ou leurs clients ou d'abuser, voler ou compromettre des biens en prenant le contrôle des systèmes qui les gèrent.

L'accès privilégié contrôle généralement les aspects les fondamentaux de l'informatique. Sans contraintes, cette capacité peut s'avérer extrêmement endommagé, et pas seulement pour les systèmes informatiques sensibles d'une entrepris

La séparation des pouvoirs dans le contrôle des comptes administrateurs informatiques aide à garantir que les dossiers comptables de l'entreprise ne puissent pas être compromis pour cacher une activité irresponsable ou illégale, ou que des systèmes qui surveillent et garantissent des pratiques commerciales responsables ne puissent pas être manipulées ou perverties. Puisque ceux qui ont des accès administrateurs privilégiés peuvent créer et modifier de ces séparations dans les systèmes qui gèrent les transactions et les données commerciales sensibles, la surveillance et le contrôle des privilèges administrateurs aident à garantir que l'intégrité des définitions de la stratégie et l'application de ces séparations restent en vigueur et soient inaltérés.

Pour la sécurité

Les privilèges administrateurs sont rarement attribués à quelqu'un qui ne serait pas considéré un initié de confiance ; cependant, même les collaborateurs les plus chevronnés sur lesquels dépendent les affaires de l'entreprise peuvent devenir une menace si le privilège administrateur est détourné. Les exemples tels que le cas de Roger Duronio, administrateur système d'UBS, condamné à planter une « bombe logique » qui a endommagé les systèmes d'informations de nombreux géants de la finance, ou Terry Childs, qui a pris le contrôle du réseau « FiberWAN » des mains de la ville de San Francisco en refusant de divulguer ses autorisations administrateurs.

Les cas d'abus incluent également un nombre croissant de grandes marques et autres entités commerciales dans lesquelles des fournisseurs, tiers de confiance, qui possédaient un accès privilégié aux réseaux et aux systèmes pour divers raisons ont été compromis. Leurs comptes ont été ensuite utilisés pour s'introduire dans les données de l'entreprise.

Des pirates externes peuvent constituer une menace plus répandue qui ont pour objectif les privilèges administrateurs puisque ceux-ci permettent d'avoir un contrôle direct sur les systèmes d'informations de l'entreprise et qui gèrent des données précieuses ou des fonctionnalités sensibles. Prises ensemble, ces menaces provenant à la fois de l'extérieur mais aussi de l'intérieur met en avant la nécessité d'une sécurité plus efficace des accès administrateurs. Le « Mandiant 2014 Threat Landscape Infographic » a rapporté que 100% des infractions ont été commis en utilisant des autorisations d'initié, par un initié de confiance devenu escroc ou par un agent de menace extérieur qui avait usurpé des autorisations d'un administrateur.

Le « 2014 Verizon Data Breach Investigation Report » indique que les infractions liées aux initiés ont augmenté légèrement depuis le rapport de 2013.1 Comme l'indique le rapport du « Mandiant », les initiés ne sont pas plus malveillants mais leurs autorisations sont usurpées de plus en plus souvent. Les rapports des fournisseurs de sécurité tels que « Symantec's 2014 Internet Security Threat Report Vol. 19 » prouvent que les attaques d'hameçonnage (phishing) visant les collaborateurs clés de l'entreprise ont augmenté jusqu'à 91% par rapport à leur étude de 2013. Les pirates informatiques deviennent de plus en plus efficaces lorsqu'ils visent leurs cibles et introduisent un malware de menaces avancées et persistantes (APT) dans leur environnement.

Pour des raisons de conformité, d'assurances des sociétés et de sécurité, il est conseillé aux entreprises de déployer une visibilité et un contrôle plus granulaires pour les accès administrateurs, indépendamment de la nature du système (Unix, Linux ou Microsoft Windows) pour les systèmes d'exploitation et les environnements applicatifs aussi bien dans des centres de données physiques que dans le Cloud.

… mais un véritable avantage pour les affaires

En plus des raisons citées ci-dessus, les entreprises devraient considérer la gestion des identités à privilèges comme un moyen d'éviter ou de réduire les coûts Reduzierung der IT-Kosten

En améliorant la fiabilité du réseau informatique

- **Personnel autorisé…** mais changement non autorisé : beaucoup d'entreprises adoptent des processus de configuration et de contrôle du changement afin de réduire au minimum les coupures de service dues aux modifications sur le réseau informatique ; mais la plupart du temps un certain nombre de facteurs contribuent à l'activité administrateur en dehors des contrôles de changement autorisé. Les urgences et les besoins pressants, les collaborateurs qui sont ignorants des contraintes de changement, des erreurs simples ou, peut-être plus alarmant, ceux qui utilisent les accès privilégiés des administrateurs qui ne seraient pas connus, pour ne citer que quelques exemples. Certains problèmes, comme les urgences, peuvent être entièrement accidentelles ; même les meilleurs collaborateurs font des erreurs. Ces facteurs devraient encourager les entreprises à repenser leur manière de conduire le changement. La complexité même de l'informatique rend difficile la gestion anticipée des éventuels scenarios, mais les contraintes sur les privilèges administrateurs exigés dans presque tous les cas peuvent aider les entreprises à identifier leurs problèmes, à mettre en place des contrôles granulaires sur les changements sur le réseau lorsque nécessaire, mais également à maintenir une visibilité élevée des activités administrateurs qui apportent assistance sur des analyses plus pointues liés aux problèmes informatiques du « root ».

1 Page 8, schéma 5

- **Personnel autorisé, changement autorisé…** mais conséquences imprévues : les administrateurs et les techniciens autorisés évaluent et déploient des modificatifs tels que prévus mais les résultats du changement ont des effets imprévus. Les changements de configuration et le déploiement de correctifs sont des exemples fréquents. Des changements peuvent être examinés mais les environnements de production peuvent avoir des nuances différentes d'une cible à l'autre. La portée du changement n'est pas forcément en corrélation avec les objectifs, ce qui génère des changements involontaires sur les systèmes d'informations ou en dehors du périmètre d'action attendu par ces changements. Les changements peuvent être en conflit avec des configurations non documentées existantes causant de l'instabilité et des pannes. Même lorsque tous les aspects des changements sont bien décrits, examinés et anticipés, parfois, ils peuvent ne pas se déployer comme prévu. Le déploiement peut être inachevé ou une défaillance dans un ordre de conditions connexes peut se produire. Les changements qui doivent être soutenus et réévalués en raison de manque de performance et de disponibilité ou de pannes représentent une part significative des dépenses en moyens informatiques. Le contrôle des accès privilégiés peut aider à les contenir grâce à la définition granulaire des cibles d'accès, des connexions des administrateurs ou la limitation et/ ou la maîtrise de l'étendue des accès privilégiés et des utilisateurs autorisés à exécuter des tâches d'administrateurs. La visibilité granulaire des accès privilégiés au sein de l'activité offre également la capacité d'identifier des dommages spécifiques dans ces cas précis.

L'étude menée par EMA soutient ces valeurs. Dans une étude basée sur plus de 200 entreprises dans le monde entier2, seulement un quart environ de l'ensemble des répondants a réalisé les quatre étapes de la méthode de gestion de la qualité ou « Plan--Do-Check-Act » (PDCA) suivantes :

- Définir les objectifs de gestion du changement (plan)
- Mettre en pratique ces objectifs (mettre en œuvre)
- Contrôler l'adhésion à ces objectifs et détecter des dérives (vérification), et enfin
- Répondre aux dérives le cas échéant (agir).

Lorsqu'on les compare aux 75% de cette étude, les plus performants ont obtenu :

- Moitié moins d'incidents liés à des événements de sécurité nécessitant une réponse non planifiée
- Moins d'incidents liés à une conduite du changement infructueuse et nécessitant une restauration du système
- Un meilleur ratio relatif à l'administration du couple serveur-système
- Davantage de projets informatiques réalisés dans le temps, dans le budget et avec les fonctionnalités attendues.

En réduisant la perte de données par la gestion des identités à privilèges

L'étude3 menée par EMA en 2014 montre que 29% des professionnels de l'informatique interrogés sont frustrés et expriment le besoin d'avoir de meilleurs outils afin d'identifier les activités telles que les abus liés aux accès privilégiés qui conduisent à une violation de données et des pannes. Trente-deux pourcent de ces mêmes professionnels de l'informatique ont déclaré que leurs entreprises ont des difficultés pour distinguer les contrôles fonctionnels des contrôles dysfonctionnels.

Quand on donne l'autorisation d'accès, la visibilité sur les accès privilégiés permet non seulement de savoir quand les administrateurs sont à l'origine des problèmes de performance du SI, du manque de disponibilité du SI ou des problèmes d'intégrité des ressources, mais également de prévenir leurs utilisations en prévoyant de façon proactive les tâches susceptibles de causer des pannes.

Lorsque l'on peut utiliser une méthode classique de contrôle et de renforcement de la politique d'audit, d'autorisation et d'authentification et qui peut être déployée à la fois pour les centres de données sur site et extérieurs au site, les coûts d'exploitation sont de ce fait davantage diminués grâce à un contrôle plus cohérent des actions des administrateurs en ayant une visibilité complète sur ces actions pour une résolution plus rapide de ces problèmes.

La gestion privilégiée des identités offre de meilleurs outils pour résoudre certains problèmes. Il surveille, impose et rend compte des contrôles qui régulent l'utilisation des accès privilégiés..

[2] *IT Risk Management: Five Aspects of High Performers that Set Them Apart*, EMA Advisory Note, juillet 2011

[3] *The Evolution of Data Driven Security*, EMA Research Report, février 2014

Lorsque l'on peut utiliser une méthode classique de contrôle et de renforcement de la politique d'audit, d'autorisation et d'authentification et qui peut être déployée à la fois pour les centres de données sur site et extérieurs au site, les coûts d'exploitation sont de ce fait réduits grâce à un contrôle plus cohérent des actions des administrateurs en ayant une visibilité complète sur ces actions et pour une résolution plus rapide ces problèmes.

- **Autorisation de l'identité…mais une utilisation, un accès aux données et une exfiltration non autorisée :** une fois dans l'environnement, les malware utilisent l'identité d'une victime pour se déplacer latéralement au sein de l'environnement afin d'effectuer une reconnaissance, de fournir un accès internet à des agents de menace extérieurs puis pour finir effacer des données. Ces activités ont un impact direct sur l'augmentation de la maintenance du SI et des coûts associés. Encore pire, lorsque les données des clients sont concernées, ces attaques génèrent des millions en coûts de nettoyage et de communication. Selon l'étude intitulée « 2014 IBM/Ponemon Cost of Data Breach Study », le coût moyen par dossier s'élève à 145 dollars U.S. par attaque et le coût total moyen est estimé à 3,5 millions de dollars U.S. En 2014, les coûts de nettoyage de certaines attaques sur des grandes enseignes américaines étaient estimés entre 4 millions et un peu plus de 100 millions de dollars U.S.. La perte de revenu pour ces marques s'élève entre environ 40 millions de dollars à un peu plus de 1 milliard. Les entreprises devraient reconnaître l'utilité de la gestion des identités à privilèges dans la réduction des coûts par le biais d'un contrôle efficace de ces privilèges, la surveillance et la communication des informations lorsque des identités sont employées de manière frauduleuse.

Les caractéristiques d'une solution efficace

Que doit comporter une solution efficace pour traiter ces problèmes ? Et comment les techniques de gestion des accès privilégiés peuvent-elles aider à réduire les coûts d'exploitation du SI et les pertes de revenu grâce à une meilleure responsabilisation des entreprises ?

Une approche complète devrait permettre :

- Aux entreprises de définir un certain nombre de paramètres souples pour contrôler les accès administrateurs tels que des créneaux horaires, des restrictions pour des individus spécifiques ou des cibles d'accès particulières mais également limiter l'accès à des utilitaires ou des fonctions spécifiques nécessaires pour certaine tâche.
- De consolider des identités en créant une personne « identité unifiée » pour l'ensemble des systèmes d'exploitation et environnements hétérogènes. Ceci améliorera le suivi et réduira la durée de vérification et de temps et les analyses criminalistiques.
- De relier le contrôle des accès utilisateurs aux systèmes, aux applications et aux services critiques grâce à une identité spécifique pour chaque utilisateur. Ceci engendre la mise en relation des comptes administrateurs, qui sont souvent mis en commun dans un groupe d'experts, et la responsabilité individuelle de chacun qui permet d'améliorer, à la fois, la granularité de la visibilité et du contrôle.
- D'offrir une efficacité en élevant les fichiers d'identités existants sans modification de schéma dans le but de maintenir une infrastructure classique et de définir les utilisateurs individuels et les comptes administrateurs. D'obtenir la capacité de développer ces ressources à travers une diversité de cibles au sein d'une entreprise hétérogène dans le but d'unifier l'identité des utilisateurs de l'entreprise, ce qui est un autre avantage.
- De fournir un audit et un suivi évolutifs, consultables et complets sur l'activité des utilisateurs dans les systèmes sensibles, y compris d'avoir la capacité de refaire la ligne de commande et les sessions utilisateurs graphiques (« reprise vidéo »).
- De centraliser la visibilité et le contrôle des privilèges par le biais d'un « point unique » pour la gestion, l'application de la politique, le suivi sur l'ensemble des serveurs et des utilisateurs.
- Ceci augmente l'efficacité (qui aide à réduire davantage les coûts) et fournit une approche unifiée et cohérente de la gestion pour un environnement donné.

- D'intégrer un audit des activités utilisateurs comme dans syslog et Windows Event Log Windows avec d'autres technologies de surveillance et de suivi centralisés telles que les solutions de gestion des événements et des informations de sécurité (SIEM).
- D'imposer moins de politiques de restrictions pour les accès privilégiés pour le contrôle des privilèges granulaires tout en pouvant faciliter l'élévation des accès privilégiés contrôlés dans le même temps sans devoir accorder le plein accès aux administrateurs ou aux accès root.
- De hiérarchiser tout en gérant des dizaines de milliers d'identités à travers des systèmes d'exploitation hétérogènes qui assistent des dizaines de milliers de systèmes.

La vision d'EMA

On dit souvent « qu'avec le pouvoir viennent les grandes responsabilités. » La gestion des accès privilégiés est le parfait exemple. Les comptes administrateurs peuvent avoir un impact considérable sur les systèmes d'informations sensibles des entreprises et les fonctions qui affectent non seulement les entreprises elles-mêmes mais également leurs clients et leurs revendeurs.

La gestion des identités à privilèges engendre l'exposition à des risques comportant des contrôles granulaires sur l'identité et l'objectif des personnes qui exercent leurs droits administrateurs mais également sur le moment où elles les exercent et la manière dont elles les exercent. Les audits des comptes à privilèges décrivent la manière dont ce pouvoir a été exercé. Lorsqu'utilisé de façon responsable, il détaille la façon dont les SI ont pu interagir pour pointer des problèmes de disponibilité de service. Lorsqu'il est utilisé de façon frauduleuse, le contrôle des privilèges aide à réduire au minimum les risques tandis que l'audit des privilèges peut documenter les actions afin d'aider à maîtriser les incidents et à fournir une application juste et responsable.

L'impact des accès à privilèges dans le SI, même utilisé de façon responsable, ne doit pas être négligé. Avec une approche moderne de la gestion et la visibilité des accès privilégiés, les entreprises peuvent respecter davantage la réglementation, aider à mieux garantir l'intégrité de l'entreprise mais également éviter les risques liés à la sécurité tout en réalisant des économies et autres et obtenir une meilleure fiabilité de leur système d'informations.

L'impact des accès à privilèges, même utilisés de façon responsable, ne peut être négligé. Avec une approche moderne de la gestion et la visibilité des accès privilégiés, les entreprises peuvent respecter davantage la réglementation, aider à mieux garantir l'intégrité de l'entreprise mais également éviter les risques liés à la sécurité tout en réalisant des économies et autres et obtenir une meilleure fiabilité de leur système d'informationsren.

A propos de Centrify

Centrify fournit une gestion unifiée des identités à travers le data center, le Cloud et les environnements mobiles en utilisant l'authentification unique (SSO) pour les utilisateurs et une infrastructure des identités simplifiées pour l'informatique. Le logiciel de gestion de l'identité numérique en tant que service (IDaaS) de Centrify permet aux solutions de gestion de l'identité déjà existantes d'utiliser l'authentification unique, l'authentification multi-facteurs, la gestion des privilèges selon l'identité de l'utilisateur, les audits selon le niveau des utilisateurs et la gestion sécurisée des appareils mobiles de l'entreprise. Les clients de Centrify peuvent ainsi réduire le coût total de la gestion de l'identité et être en conformité à plus de 50 pour cent, tout en apportant une souplesse opérationnelle accrue et une meilleure sécurité d'ensemble. Centrify est utilisé par plus de 5 000 clients à travers le monde, incluant presque la moitié des entreprises du classement « Fortune 50 » et plus de 60 agences fédérales. Pour plus d'informations, veuillez consulter le site : http://www.centrify.com/

A propos d'Enterprise Management Associates, Inc.

Fondé en 1996, Enterprise Management Associates (EMA) est l'un des principaux analystes financiers du marché qui fournit une vision approfondie des technologies de gestion des SI et des données parmi l'ensemble de celles existantes. Les analystes d'EMA s'appuient sur la combinaison des expériences terrains avec leur vision des meilleures pratiques commerciales d'un secteur d'activités et la connaissance détaillée des solutions actuelles et futures des fournisseur afin d'aider les clients d'EMA à atteindre leurs objectifs. Pour en savoir davantage sur les études, les analyses et les services de conseil d'EMA pour les utilisateurs de la branche Entreprises, les professionnels du SI et les fournisseurs informatiques, veuillez consulter le site : www.enterprisemanagement.com ou blogs.enterprisemanagement.com. Vous pouvez également suivre EMA sur Twitter Facebook ou LinkedIn.

Adresse du siège social de l'entreprise :
1995 North 57th Court, Suite 120
Boulder, CO 80301
Téléphone : +1 303.543.9500Fax : +1 303.543.7687 - www.enterprisemanagement.com

2685.020515