LIVRE BLANC | AVRIL 2016

Fermez les portes dérobées au niveau du réseau

Cinq meilleures pratiques pour maîtriser les risques liés aux tiers

Dale R. Gardner
CA Security Management

ca technologies

Table des matières

Résumé

Défi

Target, Home Depot, eBay, le Bureau de gestion du personnel des États-Unis... Les incidents de sécurité majeurs subis par ces organisations (et d'autres) récemment sont survenus suite au vol ou à la compromission des informations d'identification d'un utilisateur à forts privilèges qui disposait d'un accès étendu à des systèmes sensibles. Dans près de deux tiers des cas, la violation initiale a été facilitée par la faiblesse des pratiques de sécurité mises en place par un tiers, fournisseur ou partenaire commercial, qui avait accès à un réseau interne. C'est en volant les informations d'identification de ce tiers que les attaquants ont été en mesure d'exploiter les infrastructures informatiques des entreprises visées, pour y localiser des comptes à forts privilèges qu'ils ont ensuite utilisés pour accéder à des systèmes critiques et leur porter atteinte.

Solution

Comme les organisations touchées par ces incidents, la plupart des entreprises entretiennent des relations avec un mélange complexe de fournisseurs, sous-traitants et partenaires commerciaux tiers, qui disposent chacun d'un accès spécifique à leurs infrastructures informatiques et de comptes à forts privilèges grâce auxquels ils peuvent exécuter des applications stratégiques. Dans une ère où tout est interconnexion, il n'est pas envisageable de bloquer tout accès et de supprimer les comptes à forts privilèges. La seule option possible consiste en conséquence à renforcer la protection des comptes à forts privilèges contre les utilisateurs non autorisés, de manière à mieux protéger les informations sensibles de l'entreprise.

Avantages

L'entreprise interconnectée réalise des économies et améliore la qualité de ses produits et services ainsi que ses performances en faisant appel à des entreprises tierces. Dans ce contexte, elle ne peut plus restreindre l'accès à son réseau par le biais d'un pare-feu : pour tirer les bénéfices métier de ses partenariats avec d'autres entreprises, elle doit leur donner accès aux ressources pertinentes. Pour ce faire, elle doit mettre en œuvre des meilleures pratiques en matière de sécurité des informations, afin de prévenir les violations tout en autorisant les activités métier légitimes de ses partenaires.

Section 1

Risques liés aux accès par des tiers

Aujourd'hui, il n'est pas rare que des personnes extérieures à une entreprise disposent d'un accès à forts privilèges à tout ou partie de ses réseaux et systèmes internes. Souvent, l'équipe de sécurité des informations de l'entreprise sait très peu de choses sur ces personnes, à l'exception du fait qu'elles travaillent pour des sous-traitants, des fournisseurs de services d'externalisation ou des partenaires métier de l'entreprise. Or, ces utilisateurs tiers représentent la source de risque la plus importante pour l'entreprise, car leurs comptes sont souvent le chemin le plus facile pour atteindre ses systèmes. Les incidents majeurs de sécurité les plus récents (Target, Home Depot et d'autres) en sont une très bonne illustration : en compromettant l'accès utilisateur même restreint d'un tiers, un pirate peut s'ouvrir un accès étendu aux réseaux et systèmes d'une entreprise, avec des dommages exponentiels à la clé. En outre, ce type de violations n'est pas rare : d'après Troy Leach, Directeur de la Technologie du Conseil des normes de sécurité PCI, près de 65 % des violations de sécurité subies par des entreprises sont liées à des tiers.

Conscientes de ces risques, les autorités de réglementation travaillent avec l'industrie afin de développer des contrôles et des réglementations appropriés pour répondre à ce défi. Ainsi, la version 3 de la norme de sécurité des données PCI a introduit de nouveaux contrôles visant à limiter les risques liés aux tiers. D'après Benjamin Lawsky, surintendant des services financiers pour l'État de New York, **« l'efficacité de la cybersécurité d'une banque se mesure à l'efficacité de la cybersécurité de ses fournisseurs. Malheureusement, ces entreprises tierces peuvent aussi fournir une porte dérobée aux attaquants qui cherchent à voler les données sensibles des clients de la banque. »** Face à ce danger, les autorités de réglementation des secteurs financier, de la santé et d'autres industries développent de nouvelles normes de conformité visant à réduire les risques et à améliorer le niveau de sécurité.

> « L'efficacité de la cybersécurité d'une banque se mesure à l'efficacité de la cybersécurité de ses fournisseurs. Malheureusement, ces entreprises tierces peuvent aussi fournir une porte dérobée aux attaquants qui cherchent à voler les données sensibles des clients de la banque. »
>
> – Benjamin Lawsky, surintendant des services financiers, État de New York

---

Section 2

Cinq meilleures pratiques pour maîtriser les risques liés aux tiers

Être en mesure de contrôler et de gérer l'accès des tiers à ses réseaux et systèmes est une exigence de plus en plus importante pour toute entreprise, pour garantir la bonne gestion des risques de sécurité des informations, mais aussi sa mise en conformité par rapport aux réglementations.

> « Les pirates ont volé les informations d'identification du sous-traitant KeyPoint Government Solutions, ce qui leur a permis d'accéder aux réseaux du Bureau de gestion du personnel des États-Unis (OPM). »
>
> « Exclusive: The OPM breach details you haven't seen », 21 août 2015

Meilleure pratique n° 1 : mettre en œuvre des contrôles et des processus de support

Comme pour la plupart des problèmes de sécurité des informations, la définition de processus et contrôles visant à gérer le risque est un bon point de départ, en particulier dans le contexte d'un risque lié à des tiers dont la majeure partie des activités se déroulent en dehors du champ de supervision et de contrôle de l'équipe de sécurité des informations. Étant donné que de nouvelles relations métier peuvent s'établir et des accès être octroyés sans que l'équipe de sécurité des informations n'en ait connaissance ou ne l'ait approuvé au préalable, il est nécessaire d'impliquer cette dernière dans les négociations des contrats, de façon à garantir l'élaboration, la mise en place et l'intégration de règles de sécurité appropriées dans l'infrastructure globale de gestion des identités et des accès de l'entreprise.

Le provisioning, le déprovisioning et la définition de règles appropriées pour les utilisateurs à forts privilèges extérieurs à l'entreprise constituent la partie simple du processus. Comme pour d'autres utilisateurs à forts privilèges, il convient de répondre aux questions suivantes :

- Définition et formation des utilisateurs
- Systèmes et ressources auxquels l'accès est nécessaire
- Niveau de privilège nécessaire pour l'accomplissement des différentes tâches
- Restrictions devant être mises en œuvre
- Supervision, enregistrement des sessions, alertes et fréquence de l'examen des sessions

La plupart des entreprises ont déjà mis en place ce type de règles pour leurs utilisateurs à forts privilèges. Si ce n'est pas le cas dans votre entreprise, il convient de les créer. Les processus et contrôles appliqués aux utilisateurs à forts privilèges au sein de l'entreprise doivent aussi l'être pour les utilisateurs à forts privilèges extérieurs à l'entreprise. Selon sa structure et sa taille, ces processus pourront relever de la production IT, des responsables de la gestion des identités ou encore d'un sous-traitant. Ces groupes doivent connaître et accepter les processus de formation, de provisioning, de supervision et de déprovisioning des utilisateurs à forts privilèges tiers.

Normes de sécurité

En règle générale, la sécurité d'un système n'est jamais plus élevée que celle de son maillon le plus faible. En octroyant un accès à forts privilèges à un partenaire, l'entreprise fait de l'infrastructure et des processus de ce partenaire des composants à part entière de sa propre infrastructure IT. Dès lors, il suffit qu'un partenaire présente des systèmes de contrôle ou de sécurité insuffisants pour ouvrir une brèche dans la protection de l'entreprise : l'incident de sécurité subi par le Bureau de gestion du personnel des États-Unis suite au vol des informations d'identification de l'un de ses sous-traitants, KeyPoint Government Solutions, l'a clairement démontré. Pour garantir la gestion des risques, il est donc essentiel d'évaluer les mesures de sécurité de chaque partenaire par rapport aux normes établies. De plus en plus, les normes PCI, HIPAA et d'autres imposent de nouvelles exigences sur la base desquelles les performances des fournisseurs tiers doivent être évaluées.

La plupart des entreprises ont déjà mis en place des normes de sécurité des informations, lesquelles doivent s'appliquer aux fournisseurs tiers. Pour développer une nouvelle norme de sécurité des informations, différentes sources sont disponibles :

- Le document « Standard Information Gathering » (SIG), publié par Shared Assessments, qui facilite la normalisation du processus de collecte et d'évaluation de la sécurité des informations
- Les directives globales de gestion des risques de l'OCC (Office of the Comptroller of the Currency), avec des sections spécifiques à l'IT
- Les documents relatifs aux normes du FFIEC (Federal Financial Institutions Examination Council)
- L'outil d'évaluation des risques de sécurité (Security Risk Assessment Tool) du département américain de la santé et des services sociaux
- La norme 800-53 du NIST, qui définit des contrôles de confidentialité et de sécurité pour les systèmes d'information des agences fédérales américaines

- Les organismes nationaux de réglementations
- Les cadres de contrôle du référentiel COBIT et de la norme ISO 27002

En outre, des normes de conformité sectorielles peuvent également inclure des exigences spécifiques au travail avec des tiers :

- Norme de sécurité des données PCI
- Lois HIPAA et HITECH

Implémentation, formation et mise en application

Une fois en place, les évaluations et processus doivent être implémentés et appliqués par les équipes IT, Finance, juridique et métier qui gèrent les relations avec les fournisseurs et partenaires tiers de l'entreprise. Les éléments de base suivants doivent être inclus dans les contrats en place avec les tiers :

- Garanties : mentions exactes des règles et procédures que le fournisseur/partenaire s'engage à mettre en œuvre, y compris la vérification des antécédents et la formation de ses employés qui auront accès aux systèmes de l'organisation.
- Recours : pénalités applicables en cas de non-respect des exigences du contrat et procédures de résolution.
- Dispositions applicables en matière d'audit : contrôles et bilans disponibles pour valider la mise en conformité et la fréquence des audits.

Ces dispositions fondamentales de gestion des risques doivent être incorporées dans les étapes pertinentes du processus de sous-traitance et de mise en application. Le niveau de détail des règles et de leur mise en application varie en fonction du domaine métier, et vise l'équilibre entre risques et coûts.

Meilleure pratique n° 2 : mieux authentifier les utilisateurs

Le domaine de l'identification et de l'authentification des utilisateurs est celui qui présente le meilleur rapport entre les coûts et efforts à mettre en œuvre et le niveau de réduction du risque pouvant être atteint. Comme mentionné précédemment, environ deux tiers des incidents de sécurité sont liés à des systèmes inadéquats d'identification et d'authentification des utilisateurs tiers, y compris à la gestion (ou l'absence de gestion) des informations d'identification. Généralement, les tiers en cause sont des entreprises de plus petite taille, qui manquent de la maturité et de l'expérience de plus grandes entreprises dans le domaine de la sécurité, ce qui est souvent source de problèmes. Deux causes différentes peuvent provoquer la compromission des informations d'identification d'un utilisateur : un niveau de sécurité et une gestion des informations d'identification inadéquats, ou la divulgation par inadvertance de ces mêmes informations d'identification à la mauvaise personne.

- **Informations d'identification trop peu sécurisées :** même lorsqu'un mot de passe fort est défini, appliquer les règles de mot de passe et de durée de vie peut être fastidieux. Ces principes sont ainsi fréquemment ignorés, en particulier dans les plus petites entreprises. Imaginons, par exemple, qu'un fournisseur utilise la même paire ID utilisateur/mot de passe pour tous ses clients. Si un pirate parvient à compromettre cette paire pour un seul client, il aura la possibilité d'accéder facilement à la liste des clients du fournisseur, qui a été publiée sur le site Web du fournisseur, pour ensuite accéder aux autres organisations, les unes après les autres.
- **Divulgation malencontreuse :** d'après de récentes statistiques, le taux de réussite des attaques par hameçonnage après seulement cinq à sept tentatives est proche de 100 %. Ces statistiques illustrent le degré de sophistication qu'ont atteint les techniques d'hameçonnage et la nature humaine des utilisateurs même les plus compétents. Une seule erreur peut engendrer une compromission de sécurité, comme l'a démontré l'attaque qui a entraîné la coupure du réseau électrique ukrainien en décembre 2015. Même les partenaires métier les plus compétents peuvent être victimes d'attaques d'hameçonnage.

Pour protéger les informations d'identification permettant d'accéder aux systèmes, il convient de mettre en place une gestion et un contrôle proactifs en définissant des règles sur les éléments suivants :

- Complexité
- Fréquences des changements
- Authentification multifacteur

La mise en place d'une authentification multifacteur pour tous les tiers de l'entreprise (et utilisateurs à forts privilèges en interne) relève de la meilleure pratique. Dès lors qu'une entreprise est prise pour cible, le piratage des informations d'identification utilisées par ses fournisseurs tiers n'est plus qu'une question de temps. Par exemple, dans le cas du réseau électrique ukrainien, c'est le logiciel malveillant BlackEnergy, envoyé dans une pièce jointe infectée à un utilisateur à forts privilèges peu soupçonneux, qui a servi de vecteur d'accès initial pour collecter des informations d'identification légitimes. Le meilleur moyen d'éviter cela est d'ajouter un facteur supplémentaire au processus d'authentification. Si plusieurs options d'authentification multifacteur sont possibles, la plus efficace dépend de la combinaison entre exigences économiques, réglementaires et de conformité. Par exemple, au sein du gouvernement fédéral des États-Unis, l'usage des cartes PIV ou CAC par les utilisateurs administratifs et à forts privilèges est soumis à des exigences spécifiques. Dans d'autres environnements, d'autres options sont possibles, notamment les certificats, les jetons matériels, les jetons logiciels et les processus de vérification utilisant le téléphone portable de l'utilisateur. L'aspect économique de l'authentification multifacteur est très favorable, ce qui facilite son argumentation.

Une gestion efficace des informations d'identification utilisées par les tiers implique que leurs utilisateurs disposent d'informations d'identification individuelles, or, cette simple exigence fait rarement partie des pratiques courantes des entreprises. Souvent, au lieu de créer un compte par utilisateur, l'entreprise choisit de créer un compte par fournisseur, obligeant les employés de ce dernier à utiliser le même compte et les mêmes informations d'identification. Ce mode de fonctionnement peut certes faciliter l'administration, mais il engendre des problèmes à partir du moment où plusieurs personnes partagent un compte :

- L'authentification multifacteur est plus compliquée.
- Il est plus difficile de contrôler l'accès aux informations d'identification et leur utilisation, en particulier lorsque des personnes quittent l'entreprise ou changent de rôles. Une fuite ou un vol d'informations d'identification peut survenir très facilement.
- Lorsqu'un compte est partagé entre plusieurs personnes, il est impossible de déterminer quel utilisateur a exécuté une action donnée sur le réseau, et donc provoqué le problème.

Implémenter un processus dans lequel les informations d'identification sont émises pour chaque personne plutôt que pour un seul fournisseur permet de prévenir en grande partie ce type de problème, tout en simplifiant l'ajout et la suppression des utilisateurs. Lorsqu'un nouvel employé rejoint l'entreprise partenaire, un compte est créé, permettant l'accès aux systèmes. Ce compte et l'accès correspondant peuvent ensuite être annulés aussi vite et facilement lorsque l'employé quitte l'entreprise ou change de rôle. Une gestion des accès et une authentification performantes ne sont pas qu'une question de technologie ; elles posent aussi des problèmes de personnes, de processus et de formation qui doivent être réglés dans le cadre de la négociation des accords avec les fournisseurs et de la mise en place des processus. De leur côté, les fournisseurs doivent informer l'entreprise des changements qui interviennent au sein de leurs équipes, ce qui représente du travail supplémentaire pour eux. L'entreprise doit mettre en place des procédures afin de faciliter le reporting de ces événements. Dans l'ensemble, tous ces efforts d'administration supplémentaires se justifient, car ils contribuent à grandement renforcer les niveaux de sécurité et de contrôle. En fait, les exigences réglementaires impliquent une authentification et un contrôle des accès au niveau des personnes, car c'est à ce niveau qu'ils sont efficaces.

La dernière piste de travail dans ce domaine, qui peut être atypique pour les entreprises, implique la vérification de l'historique et de l'identité des individus tiers qui accèdent aux systèmes de l'entreprise. Une fois de plus, il s'agit de gérer le risque : le coût que cela entraîne (tant financier qu'administratif) est généralement justifié, surtout dans les environnements sensibles.

La technologie de coffre-fort permet de centraliser et d'automatiser les règles de complexité des mots de passe, les changements de mots de passe et l'intégration de systèmes d'authentification multifacteur dans une seule et même solution. Une fois une gestion efficace des informations d'identification en place, une autre meilleure pratique consiste à séparer l'authentification du contrôle des accès.

Meilleure pratique n° 3 : séparer l'authentification du contrôle des accès

Toute personne accédant à un réseau donné, quel que soit ce réseau, dispose le plus souvent d'une visibilité sur de multiples systèmes et périphériques, et potentiellement d'un accès à ces derniers. Cette seule faille est à l'origine de nombreuses violations de sécurité : Target, Home Depot, le réseau électrique ukrainien et bien d'autres. Il s'agit de violations accomplies via une chaîne de frappe, autrement dit une suite d'étapes exécutée par les attaquants (parfois de manière itérative) pour parvenir à leurs fins. Ce type d'attaque commence par l'obtention de l'accès à un réseau, souvent par la compromission des informations d'identification d'un fournisseur ou d'un tiers de l'entreprise visée. Une fois dans le réseau, l'attaquant peut rechercher des vulnérabilités ou d'autres informations d'identification dont l'exploitation lui permettra de gagner l'accès à des niveaux de privilèges de plus en plus élevés, jusqu'à atteindre sa cible ultime. C'est ainsi que le réseau électrique ukrainien a subi une coupure générale.

> « D'après les indications des trois entreprises, les pirates avaient effacé plusieurs systèmes en exécutant le logiciel malveillant KillDisk. KillDisk permet de supprimer des fichiers sélectionnés sur les systèmes cibles et de corrompre l'enregistrement d'amorçage principal, pour mettre les systèmes hors service. Il a été rapporté par la suite que dans au moins un des cas, des interfaces humain-machine (HMI) Windows incorporées dans des terminaux distants avaient également été effacées par KillDisk. Les pirates ont également mis hors service des périphériques Série Ethernet au niveau de sous-stations en corrompant leur micrologiciel. Il semble qu'ils avaient planifié des déconnexions des systèmes d'alimentation sans coupure (UPS) des serveurs via l'interface de gestion à distance des UPS. L'équipe estime que ces actions ont été réalisées en vue d'interférer avec les efforts de restauration attendus. »
>
> « Cyber-Attack Against Ukrainian Critical Infrastructure »
> Date de publication initiale : 25 février 2016

Pour rompre une telle chaîne de frappe, il peut être utile de contrôler l'accès au réseau et de le rendre plus difficile en mettant en œuvre une authentification multifacteur, des mesures décrites dans la meilleure pratique n° 2. Il est également possible d'ajouter une couche de défense supplémentaire, en limitant la visibilité et l'accès aux ressources du réseau des fournisseurs. La plupart d'entre eux ont besoin d'accéder à des systèmes très précis. Ils n'ont pas besoin d'accéder ou même de pouvoir voir l'intégralité du réseau, voire d'un sous-réseau.

La segmentation du réseau physique permet de limiter leur visibilité et leur accès au réseau. La segmentation est une opération fréquemment rendue nécessaire pour des raisons de conformité avec des réglementations. La segmentation du réseau et le contrôle des accès permettent de limiter la portée des ressources disponibles. Aussi efficace qu'elle soit, cette approche présente aussi des inconvénients :

- Coûts d'administration requis pour configurer et entretenir l'architecture réseau
- Vulnérabilité au niveau des connexions entre les différents segments du réseau : le risque est qu'un pirate trouve un moyen d'exploiter les connexions réseau pour gagner l'accès à sa cible

Utiliser une solution de gestion des identités à forts privilèges telle que CA Privileged Access Manager, pour mettre en place une segmentation logique qui permet de limiter l'accès aux ressources, constitue une meilleure alternative : cette solution implémente un « point de passage obligé » au niveau duquel tout utilisateur doit obtenir l'approbation pour pouvoir accéder aux ressources protégées de l'entreprise. Cette approche offre un certain nombre d'avantages :

- **Contrôle d'accès « confiance zéro » :** une connexion réussie ne donne pas accès au réseau entier. Au lieu de cela, des règles spécifient les ressources disponibles en fonction de l'utilisateur, limitant son accès à ces seules ressources. Cette approche rend possible un contrôle très étroit de la visibilité et de l'accès de l'utilisateur, qui ne voit jamais les ressources auxquelles il n'est pas autorisé à accéder. Il visualise uniquement la liste prédéfinie des systèmes auxquels il est autorisé à accéder.
- **Prévention des sauts :** pour contrôler les déplacements latéraux dans un réseau, le système intercepte un certain nombre de commandes d'exploration, les commandes TELNET ou SSH notamment, pour empêcher leur exécution. Cette capacité permet de limiter l'accès de tiers aux seuls systèmes prédéfinis, et les empêche de voir le reste du réseau et d'accéder à d'autres systèmes.

Il est important de normaliser et de consolider les méthodes d'accès en créant un point de passage obligé, à l'aide d'une solution de gestion des accès à forts privilèges, d'un VPN ou d'une autre solution pour canaliser les accès sur les chemins connus. La définition de chemins d'accès acceptables aux ressources pour les utilisateurs externes rend l'ensemble des tâches de supervision plus faciles. Comme les protocoles non approuvés sont contenus et les sessions approuvées redirigées vers des routes prédéfinies, il est plus facile d'identifier les anomalies pour les examiner de plus près, avec des solutions de gestion des informations et des événements de sécurité (SIEM) et des outils de journalisation qui détectent les événements anormaux.

Meilleure pratique n° 4 : prévenir les erreurs et les commandes non autorisées

Les droits et autorisations d'accès peuvent servir à limiter l'accès aux ressources IT. Parfois, cette approche n'offre pas le niveau de précision nécessaire pour véritablement contrôler ce qu'une personne fait sur un système. Par exemple, un administrateur système tiers peut avoir besoin de se connecter à un serveur en utilisant un compte root ou admin (compte de superutilisateur à forts privilèges). Si cet accès est approuvé, pour des raisons techniques ou administratives, on se retrouve alors dans une situation à risque : doté d'un tel niveau de pouvoir, l'administrateur pourrait faire à peu près tout sur le système, notamment l'effacer intégralement. Un tel risque est naturellement inacceptable pour la plupart des entreprises, même si la personne en cause est son employé.

L'approche alternative, basée sur une solution de gestion des accès à forts privilèges, est plus adaptée, dans la mesure où elle permet un contrôle fin des autorisations, et donc une meilleure gestion de ce type d'utilisateur. Dans un système de gestion des accès à forts privilèges, un utilisateur peut déléguer des sessions en son nom vers différents systèmes cibles, en utilisant des comptes (root, par exemple) présentant chacun un niveau d'autorisation différent.

Des fonctions de filtrage des commandes, de listes noires et de listes blanches permettent également de limiter les commandes pouvant être exécutées par un utilisateur spécifique. L'utilisation combinée de listes noires (répertoriant des commandes qui ne sont pas autorisées) et blanches (contenant les commandes pouvant être exécutées) assure un niveau de contrôle et de flexibilité optimal, de sorte que l'utilisateur à forts privilèges peut gérer la ressource informatique, sans risquer d'entraîner des dommages inacceptables. Le filtrage des commandes permet en outre de prévenir les erreurs inopinées. Si nous reprenons l'exemple précédent, le superutilisateur a la capacité de déplacer des fichiers, mais ne peut pas reformater le disque.

L'utilisation combinée de filtres de commandes et de la journalisation facilite la supervision et le déclenchement d'alertes, permettant au système de réagir de manière appropriée lorsqu'une personne tente de contourner l'un des filtres (en émettant un avertissement ou en mettant fin à la session du coupable). Imaginons, par exemple, qu'un utilisateur décide de tester les limites fixées par les filtres de commandes : lorsque ces limites seront atteintes, le système génèrera une alerte invitant les responsables à examiner les actions de l'utilisateur. Voici quelques-unes des actions qui pourraient survenir en réaction à cette alerte :

- Bloquer l'utilisateur et lui envoyer un avertissement
- Mettre fin à sa session
- Désactiver le compte de l'utilisateur
- Générer une alerte/alarme au niveau du SOC

Meilleure pratique n° 5 : superviser et enquêter

Il est nécessaire de maintenir une supervision à tout moment. Le degré de supervision et le champ d'action requis dépendent de vos problématiques particulières en matière de gestion des risques et de la conformité.

Même dans des situations dans lesquelles le risque intrinsèque est réduit, la journalisation facilite le dépannage et l'examen des activités suspectes. La journalisation élémentaire, qui consiste dans l'enregistrement de l'ensemble des événements, permet de réviser toute activité non appropriée ou non autorisée. Les informations enregistrées sont les suivantes :

- Heures de connexion et de déconnexion
- Systèmes auxquels l'utilisateur a accédé
- Commandes émises
- Réponses reçues

Lorsque la situation est sensible, la supervision est complétée par l'exploitation de journaux afin d'appliquer des règles établies de contrôle de l'accès aux systèmes. Différentes actions peuvent être entreprises en réponse à une tentative de violation des règles : à un niveau élémentaire, toute tentative de violation appelle une investigation afin de déterminer ce qui s'est passé. Une formation supplémentaire peut être requise pour aider les personnes à comprendre les tâches qui sont attendues d'elles et comment ces tâches doivent être exécutées. Une violation peut découler d'une simple erreur ou bien être le symptôme d'un comportement malveillant. La supervision permet de détecter les événements douteux afin de les examiner.

Ces efforts d'investigation sont très importants, comme le montre l'affaire de la banque JPMorgan Chase, dont les équipes ont découvert que ses systèmes avaient subi une violation de sécurité après avoir enquêté sur l'un de ses fournisseurs.

« JPMorgan a découvert la présence de pirates dans ses systèmes en août, après avoir dans un premier temps constaté que ces mêmes individus avaient réussi à franchir la sécurité d'un site Web d'une course de charité sponsorisée par la banque… C'est seulement après cela que les équipes de JPMorgan se sont rendu compte que les pirates s'étaient aussi attaqué à son réseau. »

« Neglected Server Provided Entry for JPMorgan Hackers »
The New York Times, 22 décembre 2014

Lorsque la situation est encore plus critique, l'enregistrement ou la capture de sessions peut fournir les informations complètes sur ce qui s'est passé au cours d'une session donnée, ce qui aidera les enquêteurs pour la suite. La capture des enregistrements des sessions sensibles en plein écran est une pratique courante. Si des violations ou problèmes sont détectés par la suite, l'examen de ces enregistrements permet d'évaluer ce qui s'est passé dans la session initiale. Selon la sensibilité de l'environnement, il peut être utile de procéder à des contrôles ponctuels. Cependant, l'un des défis généralement associés à l'enregistrement de sessions réside dans la taille de ces enregistrements (et la charge système en résultant), qui peut être très importante. L'autre défi consiste à établir un plan d'action pour réviser les sessions enregistrées : comme les coûts liés au temps et à la technologie augmentent en cas d'enregistrement, une analyse coûts/bénéfices permet de déterminer les situations dans lesquelles ce niveau d'investissement est approprié. En point de départ, il est utile d'identifier les éléments suivants :

- Quand enregistrer et pendant combien de temps ?
- Quand réviser les enregistrements et à quelle fréquence ?
- Quelle politique de conservation appliquer pour les enregistrements ?

Si vous choisissez de déployer des techniques d'enregistrement de sessions, veillez à disposer des fonctionnalités suivantes :

- Accès facile aux métadonnées sur la session (quand elle a commencé et pris fin)
- Possibilité de parcourir rapidement les sessions, pour accéder à un moment spécifique dans un enregistrement
- Capacité à pointer une activité « intéressante », la violation d'une règle ou une activité sensible par exemple

Les situations présentant le niveau de risque le plus élevé peuvent justifier une supervision « par-dessus l'épaule » ou un accès par deux parties : dans ce cas, une personne supplémentaire devra « regarder » ce qu'un utilisateur à forts privilèges fait en temps réel. Généralement, ces situations présentant un niveau de risque extrême ne concernent pas des tiers ou autres utilisateurs externes. La supervision « par-dessus l'épaule » pose plusieurs défis d'ordre technique. En outre, le superviseur doit être hautement compétent et comprendre les actions entreprises et leurs ramifications à une échelle étendue. La supervision « par-dessus l'épaule » se justifie dans un nombre très limité de situations.

Une supervision plus typique implique un processus en deux étapes :

- **Réponse en temps réel aux violations des règles :** plusieurs actions peuvent se produire (envoi d'une alerte à l'utilisateur, génération d'une alerte vers un centre opérationnel de sécurité ou fermeture d'une session ou d'un compte).
- **Recherche et analyse après les faits :** révision des journaux ou des enregistrements de sessions pour permettre le dépannage ou une enquête.

Ces recherches et analyses peuvent inclure un travail de corrélation entre les journaux et les alertes générées par un système de gestion des accès à forts privilèges avec d'autres outils réseau et de sécurité pour les événements inattendus. Par exemple, dans les entreprises dans lesquelles une solution de gestion des accès à forts privilèges est déployée, toute l'activité d'administration est centralisée dans le système de gestion des accès à forts privilèges. Si des demandes de session SSH ou TELNET proviennent d'autres parties du réseau, elles génèrent immédiatement des alertes et font l'objet d'une enquête. Les outils d'administration non autorisés étant éliminés ou interdits, l'identification des activités suspectes devient relativement facile. Un pare-feu de nouvelle génération peut aider à marquer les applications ou protocoles qui sont interdits. L'accès à des heures inattendues ou un comportement inhabituel, comme le téléchargement de fichiers, sont d'autres activités qui peuvent être considérées comme suspectes.

Avec le temps, les audits et révisions manuels continus aident à affiner les outils et les règles pour ignorer les faux positifs et automatiser les déclencheurs et alertes, et ainsi gagner en efficacité.

Section 3 :

Avantages de la gestion des risques liés aux tiers

Aucune entreprise moderne ne saurait s'isoler et se déconnecter d'Internet : toute relation d'affaires qu'elle entretient nécessite une collaboration électronique avec son partenaire, au cours de laquelle des informations sensibles sont échangées. Aujourd'hui, les entreprises font appel à des prestataires tiers pour leurs services de comptabilité, de traitement des paiements, de conseil légal, de gestion des plans de retraite, de marketing, de fabrication et bien d'autres services. La collaboration électronique entre l'entreprise et ses partenaires métier lui permet de gagner du temps et de l'argent, et d'automatiser ses processus et systèmes pour gagner en précision, en qualité et en efficacité. Dans ce contexte, limiter l'accès à son réseau au niveau du pare-feu n'est plus possible. Pour tirer les bénéfices métier de ses partenariats avec d'autres entreprises, elle doit leur donner accès aux ressources pertinentes. Dans le même temps, toute connexion avec des tiers engendre des risques réels.

Les violations de sécurité peuvent coûter cher. Suite au vol de 40 millions de numéros de cartes de paiement et de près de 70 millions d'autres données dans ses systèmes fin 2013, la chaîne de magasins Target estimait ses pertes financières à 162 millions de dollars après dédommagement par les compagnies d'assurance (source : magazine Fortune). De son côté, Sony a dû dépenser 35 millions de dollars pour restaurer ses systèmes financiers et informatiques après l'attaque subie en 2014. Pour Home Depot, la facture s'est élevée à 28 millions de dollars avant impôts. Ces coûts ne rendent pas compte des dommages en termes de réputation et de hausse des primes d'assurance, ni des bouleversements que de tels incidents provoquent dans la vie de certaines personnes. Des personnes ont perdu leur emploi et d'autres ont dû travailler d'arrache-pied pour enquêter et résoudre les violations.

> « Quelle que soit la façon dont nous l'envisagions et que nous regardions vers le passé ou l'avenir, le constat est sans équivoque : les entreprises doivent investir dans la sécurité de leurs informations. »
>
> Benjamin Dean, universitaire de la School of International and Public Affairs de la Columbia University Magazine Fortune, 27 mars 2015

Aucune entreprise ne souhaite faire la une du Wall Street Journal en tant que victime d'un incident majeur de sécurité. Les cinq meilleures pratiques en matière de sécurité des informations décrites dans ce document visent à les aider à prévenir de telles violations, tout en leur permettant de poursuivre leurs activités métier légitimes et en préservant la sécurité de leurs informations et leur réputation.

Section 4 :

Conclusions

D'après le rapport 2015 « Data Breach Investigations Report » (DBIR) de Verizon, ce sont près de 700 millions d'enregistrements de données qui ont été compromis en 2015, soit une perte financière estimée à 400 millions de dollars. Les 70 entreprises qui ont contribué à ce rapport ont signalé 79 790 incidents de sécurité au total, dont 2 122 violations confirmées dans 61 pays (et les 2/3 aux États-Unis). Bien que la grande majorité des menaces proviennent de sources externes, les menaces liées aux partenaires et celles venant de l'intérieur même des entreprises ont connu une légère augmentation entre 2013 et 2014. Les risques sont réels, comme le montre la violation de sécurité subie par le Bureau de gestion du personnel des États-Unis (OPM).

La chaîne de frappe utilisée dans le cadre de cette attaque contre l'OPM était la suivante : ciblage d'un sous-traitant dans le cadre d'une attaque d'ingénierie sociale et vol de ses informations d'identification afin d'obtenir l'accès au réseau ; introduction d'un logiciel malveillant sur un système et création d'une porte dérobée ; exfiltration non détectée de données sur une période de plusieurs mois.

Cette violation de la sécurité de l'OPM montre combien les organisations sont vulnérables face aux techniques d'ingénierie sociale. Les employés et sous-traitants du gouvernement fédéral suivent désormais des programmes de sensibilisation à la sécurité, dans le cadre desquels ils apprennent les dangers des attaques par hameçonnage et autres menaces provenant des réseaux sociaux.

> « The most innovative and damaging hacks of 2015 »,
> CSO Magazine, 28 décembre 2015

Il est possible de minimiser de nombreux risques en appliquant les cinq meilleures pratiques décrites dans ce document. Combinées, ces pratiques permettent de créer un système de défense des informations à plusieurs couches plus robuste, plus flexible et plus puissant. En voici le détail :

- Mettre en œuvre des contrôles et des processus de support qui définissent et appliquent les règles d'accès pour les utilisateurs tiers à forts privilèges.
- Mieux authentifier les utilisateurs en appliquant une technologie d'authentification multifacteur, afin que les informations d'identification des utilisateurs à forts privilèges soient plus difficiles à compromettre, même dans le cas d'attaques par ingénierie sociale et hameçonnage.
- Séparer l'authentification du contrôle des accès, afin que les utilisateurs à forts privilèges n'aient qu'une visibilité limitée sur les réseaux internes, et ainsi réduire les dommages qu'un seul utilisateur (ou un seul jeu d'informations d'identification volées) peut infliger.
- Empêcher les erreurs et les commandes non autorisées de manière à ce que des déclencheurs en temps réel fassent office de première ligne de défense, pour protéger l'infrastructure des erreurs et activités malveillantes.
- Superviser l'activité et enquêter sur tout événement suspect, afin de détecter rapidement une éventuelle violation, d'améliorer la formation lorsque cela est nécessaire et d'affiner constamment les processus et l'automatisation pour éliminer les faux positifs.

Les systèmes de gestion des accès à forts privilèges intègrent des fonctionnalités automatisées qui permettent de définir, d'automatiser et d'appliquer les cinq meilleures pratiques décrites dans le présent document à l'échelle de l'entreprise, dans ses environnements physiques, virtuels et Cloud, pour l'aider à mettre en œuvre des processus cohérents sur ses systèmes, applications et périphériques.

Section 5

Références

https://www.brighttalk.com/webcast/9017/156931

http://www.xceedium.com/solutions/privileged-identity-management/432-2

http://www.bankinfosecurity.com/occ-more-third-party-risk-guidance-a-7233/op-1

http://www.bankinfosecurity.com/banks-vendor-monitoring-comes-up-short-a-8103

Rapport du département des services financiers de l'État de New York (NYDFS) du 9 avril, « Update on Cyber Security in the Banking Sector: Third Party Service Providers »
http://www.nytimes.com/2016/03/01/us/politics/utilities-cautioned-about-potential-for-a-cyberattack-after-ukraines.html?emc=edit_tu_20160301&nl=bits&nlid=59970007

https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

http://www.cnbc.com/2015/07/22/4-arrested-in-schemes-said-to-be-tied-to-jpmorgan-chase-breach.html

« How Much do Data Breaches Cost Big Companies? Shockingly Little »
http://fortune.com/2015/03/27/how-much-do-data-breaches-actually-cost-big-companies-shockingly-little/ 27 mars 2015

http://fortune.com/tag/data-breach 2 mars 2016

http://www.crn.com/slide-shows/security/300077563/the-10-biggest-data-breaches-of-2015-so-far.htm/pgno/0/10?itc=refresh 27 juillet 2015

https://fcw.com/articles/2015/08/21/opm-breach-timeline.aspx 21 août 2015

http://www.csoonline.com/article/3018343/security/the-most-innovative-and-damaging-hacks-of-2015.html

Section 6 :

À propos de l'auteur

Dale R. Gardner possède près de vingt ans d'expérience dans le domaine des logiciels d'entreprise, des réseaux et de la gestion des systèmes, ainsi que dans divers aspects de la sécurité IT, notamment la gestion des identités, la sécurité des applications, la gestion des vulnérabilités, la mise en conformité et la sécurité réseau. Ancien analyste et auteur dans la recherche, il a conçu, créé et commercialisé diverses solutions de sécurité et de gestion destinées à améliorer le fonctionnement des systèmes et à garantir l'intégrité et la fiabilité des infrastructures informatiques des entreprises. Il est aujourd'hui responsable du marketing international chez CA Technologies, pour le portefeuille de gestion des accès à forts privilèges.