LIVRE BLANC | NOVEMBRE 2015

Rompre la chaîne de frappe

Prévention des violations de données grâce à la gestion des accès à forts privilèges

ca technologies

Résumé

Défi

Il ne se passe pas une journée sans que l'actualité soit marquée par une nouvelle affaire de violation de données, avec la perte de secrets commerciaux, de données financières ou d'informations personnelles qui en résulte. Ces incidents touchent tous les secteurs de l'économie : commerce, éducation et administrations. Le fléau de la cybercriminalité, qui représente pour l'économie mondiale un coût de plusieurs centaines de milliards de dollars par an[1], pourrait, sans une action immédiate et agressive, atteindre des trillions de dollars de coûts en moins d'une décennie[2]. En outre, l'impact est dévastateur pour les personnes ayant subi la perte d'informations extrêmement intimes sur leur vie personnelle.

Les spécialistes en matière de sécurité ont fait tout leur possible pour établir des défenses de périmètre dont le rôle est, pour simplifier, de protéger les gentils à l'intérieur et de laisser les méchants dehors. L'enchaînement ininterrompu de violations auquel nous assistons aujourd'hui semble prouver que ces périmètres de sécurité ne remplissent pas leur rôle. Les organisations s'attèlent donc aujourd'hui à la mise en place d'une nouvelle couche de sécurité essentielle, centrée spécifiquement sur la protection et la gestion des identités, une problématique critique dans les efforts actuels visant à mettre fin à cette vague de cybercriminalité. Parmi ces identités, les plus critiques sont celles des utilisateurs à forts privilèges. Étant donné qu'elles ouvrent littéralement « les portes du royaume », le vol et l'utilisation malveillante de ces informations d'identification sont le principal vecteur d'attaque de toutes ces violations.

Solution

Les équipes responsables de la sécurité ont à leur disposition un choix de technologies et de processus matures, désignés collectivement par le terme « gestion des accès à forts privilèges », qui offrent des moyens de dissuasion et des solutions pour vaincre les attaquants. Les utilisateurs malveillants, qu'ils viennent de l'intérieur ou de l'extérieur, suivent une série d'étapes logiques pour mener à bien leurs attaques. Ces séquences, initialement identifiées et définies par les équipes de cybersécurité de Lockheed Martin[3], ont été baptisées « chaînes de frappe » en référence à un terme de stratégie militaire, du fait que si la séquence d'actions (ou de frappes) lancée par les attaquants peut être interrompue à un moment donné, l'attaque finale pourra être empêchée ou limitée. La gestion des accès à forts privilèges offre les moyens nécessaires pour contrecarrer les attaquants à différentes étapes du cycle d'attaque. Dans ce livre blanc, nous allons analyser une version légèrement simplifiée de chaîne de frappe et proposer un exemple concret d'utilisation de la gestion des accès à forts privilèges pour aider à stopper les attaques et à protéger les organisations contre ces violations.

Avantages

Les avantages financiers de la prévention des violations sont évidents. Il est toutefois plus difficile de mesurer les coûts indirects, qui sont pourtant parfois plus dévastateurs, en termes d'atteinte à la marque et à la réputation, de perte de confiance de la part des partenaires et des clients, ainsi que de l'impact sur l'évaluation boursière de la société. Toutefois, aussi importants que soient ces coûts, ils sont bien pâles en comparaison de l'impact catastrophique que le vol d'informations personnelles détaillées peut avoir sur des personnes confiantes. La gestion des accès à forts privilèges, avec sa capacité à limiter ces différentes atteintes, est donc clairement essentielle.

Défi – Violations de données : escalade des risques et dommages incalculables

Dans le cadre de l'analyse de la vague d'incidents de sécurité actuelle, il est fréquemment fait mention de l'affaire Target, qui a débuté fin 2013. Avec près de 70 millions d'enregistrements de carte de paiement volés, l'incident Target ne constituait pas la première, ni même la plus importante, violation de données de l'histoire ni de l'année 2013. Cependant, du fait de divers facteurs, l'affaire Target a attiré l'attention de plusieurs instances critiques sur la nature extrêmement dommageable de ces attaques permanentes. Depuis l'affaire Target, nous avons observé d'innombrables violations, de moindre envergure et moins médiatisées, ainsi qu'un flux constant d'incidents de plus grande ampleur, notamment avec les affaires Home Depot et JP Morgan Chase environ un an plus tard et, plus récemment, la violation des données personnelles extrêmement sensibles de près de 15 millions de clients T-Mobile de la société Experian.

> « Pour les entreprises numériques, la gestion des identités à forts privilèges est devenue aussi cruciale que complexe. Cruciale, car un administrateur doté de mauvaises intentions ou le vol des identifiants d'un administrateur peuvent avoir des conséquences désastreuses sur vos clients, votre chiffre d'affaires et votre réputation sur le long terme. »
>
> —Forrester Research[4]

Le coût de la cybercriminalité en 2014 a été estimé à près de 400 milliards de dollars, selon les données fournies par Intel Security et le Center for Strategic and International Studies (CSIS). Il peut être difficile d'appréhender des chiffres aussi énormes. Pour mieux comprendre, comparez avec la part du trafic de drogues mondial, qui est estimée à « seulement » 300 milliards de dollars par an. Le coût de la cybercriminalité est même plus élevé que le PIB de nombreux pays prospères, comme par exemple Singapour, avec quelque 300 milliards de dollars par an. Il s'agit là clairement d'un problème financier majeur, et les données recueillies suggèrent qu'en l'absence d'une action rapide, la situation ne fera que s'aggraver. Ainsi, McKinsey prévoit un impact annuel mondial de 3 billions de dollars dans 10 ans.

Ces incidents sont donc clairement préjudiciables. Les entreprises ayant connu des violations et d'autres organisations similaires ont subi une perte de capitalisation boursière, de ventes, de clientèle et de profits. Sans parler des dommages financiers et émotionnels pour les individus affectés par ces violations, qui subissent les ravages de crimes tels que le vol d'identité. Cependant, aussi inquiétants que soient ces faits, la situation s'aggrave encore si nous tenons compte des incidents survenus plus récemment.

Tout d'abord, nous avons pu observer des attaques clairement destinées à avoir un impact matériel au niveau du fonctionnement des organisations ciblées. Vous n'avez peut-être jamais entendu parler de Code Spaces, une petite entreprise basée au Royaume-Uni et proposant des services Cloud de sauvegarde et de contrôle de version pour les développeurs. En juin 2014, un pirate informatique a réussi à obtenir des identifiants administrateur pour accéder à la console de gestion AWS (Amazon Web Services) de Code Spaces. Après avoir créé de nombreux comptes et portes dérobées, le pirate a présenté à la direction de Code Spaces une demande de rançon. Le temps que les administrateurs légitimes tentent de chasser le pirate de leur système, il était déjà trop tard. Doté de droits d'administration complets, le pirate avait accédé à l'ensemble du système de gestion de Code Spaces et riposté en détruisant rapidement toute l'infrastructure informatique de l'entreprise : serveurs, applications et, plus dramatique encore, les sauvegardes de données et systèmes. L'attaque a été menée en quelques heures. En quelques jours, l'entreprise a été forcée de cesser son activité[5]. L'attaque de Code Spaces est un exemple dramatique, mais de nombreuses autres affaires illustrent cette nouvelle tendance (par exemple Sony Pictures Entertainment et Saudi Aramco).

De là, il ne manque qu'un pas pour arriver à la dernière tendance en date, à savoir le cyberespionnage. Les prémices de ces attaques ont été des violations de sécurité dans des compagnies d'assurance, notamment Anthem, Premera et CareFirst, début 2015. Bien que ces atteintes à la sécurité n'aient jamais été officiellement attribuées à des États-nations, la rumeur la plus répandue est que ces vols de millions de fichiers de données personnelles feraient partie d'une campagne plus vaste visant à constituer des dossiers sur les personnes occupant des postes clés au sein des gouvernements, des prestataires du secteur de la défense, des entreprises du secteur de la finance et des télécommunications, ainsi que parmi les décideurs géopolitiques et autres acteurs de même ordre. Le moment où ces attaques ont eu lieu semble coïncider avec la diffusion d'une alerte confidentielle, de la part du FBI, concernant l'existence de pirates informatiques chinois cherchant à obtenir des informations d'identification personnelle sur les réseaux commerciaux et gouvernementaux américains[6]. Depuis lors, bien entendu, nous avons appris l'attaque qu'a subie l'organisme américain OPM (Office of Personnel Management), durant laquelle des données personnelles, et notamment des informations biographiques, financières, personnelles et d'emploi ont été dérobées.

Solution - Comptes à forts privilèges : la nouvelle première ligne

Arrêtons-nous un instant et résumons : les violations de données constituent aujourd'hui un problème considérable, qui ne cesse de prendre de l'ampleur. Les enjeux ne cessent de croître et les adversaires auxquels nous devons faire face sont de plus en plus sophistiqués, et bien financés. Nous ne pourrions blâmer le plus optimiste des lecteurs s'il devait ressentir une pointe de pessimisme, à la lecture de ce bilan morose. Que faire face à un tel défi ?

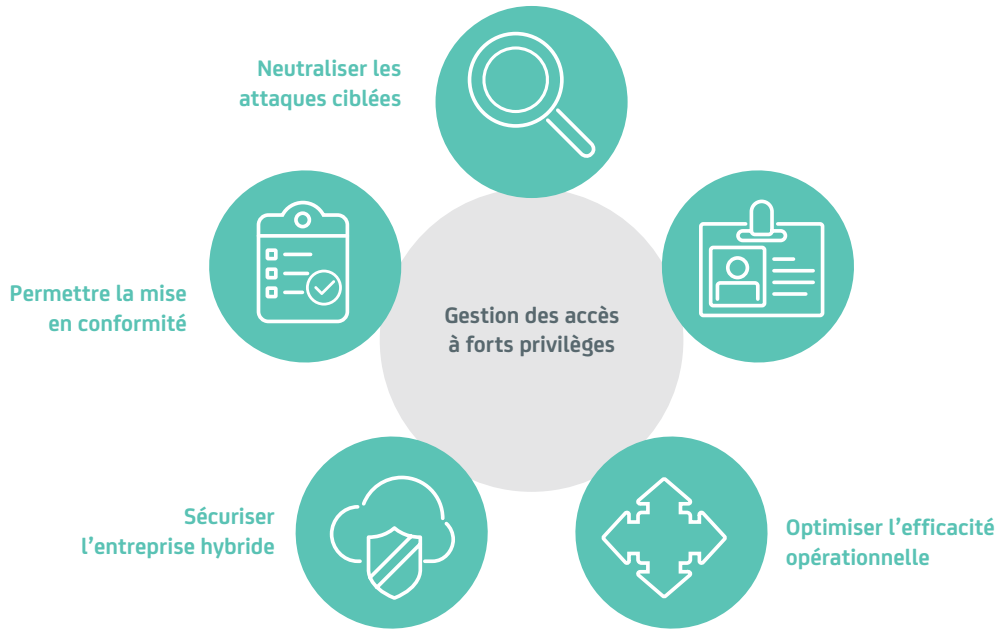


Illustration A.

La gestion des accès à forts privilèges aide les organisations à atteindre cinq objectifs clés.

La bonne nouvelle est que nous avons des raisons d'espérer ; en effet, toutes ces attaques semblent avoir un fil commun. Ce fil commun, ce sont les utilisateurs à forts privilèges et, plus spécifiquement, les données d'identification et les comptes à forts privilèges dont ces utilisateurs se servent pour assurer la configuration, la maintenance et l'exploitation de nos infrastructures IT. Le vol ou l'utilisation malveillante de ces données d'identification, qui offrent un accès privilégié aux infrastructures IT, s'est avéré jusqu'ici un facteur de succès critique et un vecteur d'attaque majeur pour les pirates, dans toutes les affaires de violation de sécurité dont nous avons parlé précédemment.

> « D'ici 2018, l'incapacité des organisations à définir et à contenir les accès à forts privilèges sera responsable de plus de 60 % des menaces internes et des vols de données, contre 40 % aujourd'hui. »
>
> —Gartner[7]

Avant d'examiner le rôle central des accès à forts privilèges dans les attaques réussies, il est intéressant de découvrir rapidement qui sont ces utilisateurs à forts privilèges, en réalité bien plus nombreux que ce qui est communément admis, au même titre que les comptes et les données d'identification utilisés pour ces accès.

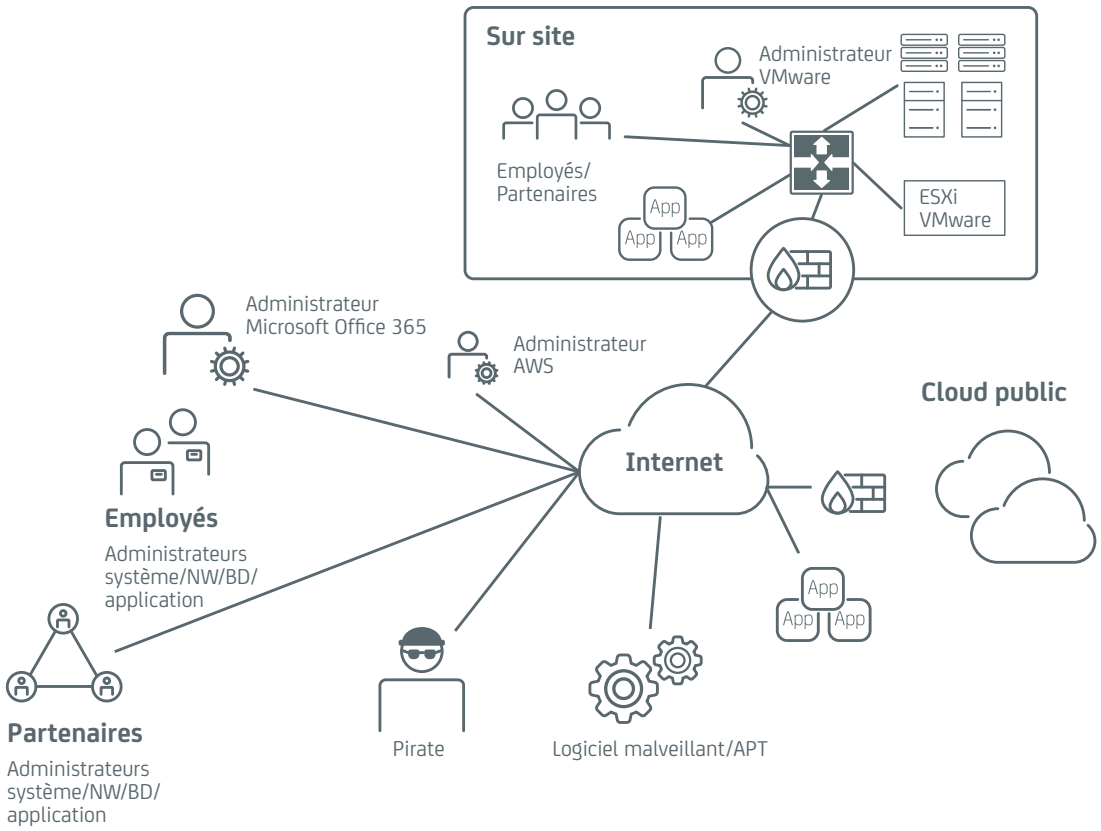


Illustration B.

Comptes à forts privilèges : la nouvelle première ligne.

Pendant des années, lorsqu'il était question d'utilisateurs à forts privilèges, seules les personnes internes à l'organisation et ayant une responsabilité concrète et directe dans l'administration du système et du réseau étaient prises en compte. Beaucoup ont ainsi sous-estimé le risque et pensent que la gestion des accès à forts privilèges se limite à maîtriser la « menace interne ». Il est vrai que les utilisateurs internes malveillants peuvent causer des dommages importants, mais de tels incidents sont relativement rares et ne constituent qu'un faible pourcentage de l'ensemble des violations.

En réalité, nombre d'utilisateurs à forts privilèges ne sont pas internes à l'organisation ; il s'agit de fournisseurs, de sous-traitants, de partenaires commerciaux ou de toute autre personne à qui des droits d'accès privilégiés aux systèmes de l'organisation ont été octroyés. Dans de nombreuses entreprises, ces utilisateurs tiers sont souvent bien plus nombreux que les utilisateurs à forts privilèges internes. L'expérience suggère également que ces tiers représentent un risque bien supérieur. Dans les affaires de violation que nous avons mentionnées (Target, Home Depot et l'OPM, entre autres), les données d'identification d'un tiers autorisé ont été compromises, puis utilisées pour obtenir un accès illicite au réseau étendu et à ses ressources.

Autre problème, le nombre d'utilisateurs à forts privilèges a augmenté avec l'adoption du Cloud et des technologies telles que la virtualisation. En ce qui concerne le Cloud, en particulier, nombre de ces utilisateurs à forts privilèges ne font en réalité pas partie de l'équipe IT traditionnelle. Prenons, par exemple, le cas de représentants métier faisant l'acquisition d'offres de service pour lesquelles, dans le pire des cas, les équipes IT et de sécurité traditionnelles n'ont aucune idée des risques associés.

Sans oublier que, de plus en plus, les utilisateurs à forts privilèges ne sont pas toujours de vrais utilisateurs, c'est-à-dire de vraies personnes. Dans les environnements Cloud et virtualisés, l'émergence d'outils de configuration et de provisioning automatisés régis par des scripts et des programmes a créé encore davantage d'« utilisateurs » bénéficiant de privilèges élevés sur de larges parties d'infrastructures. Autre problème similaire à celui des systèmes automatisés, les innombrables scripts et programmes assemblés au fil des ans et qui exigent un accès administratif ou sensible à des ressources telles que les bases de données et autres applications et systèmes. Dans ces deux cas, l'accès et les opérations effectuées sont contrôlés par authentification, de manière plutôt correcte. Malheureusement, les données d'identification requises sont généralement codées en dur dans les applications ou les fichiers de configuration, où elles constituent une cible facile pour les utilisateurs malveillants, qu'ils soient internes ou externes.

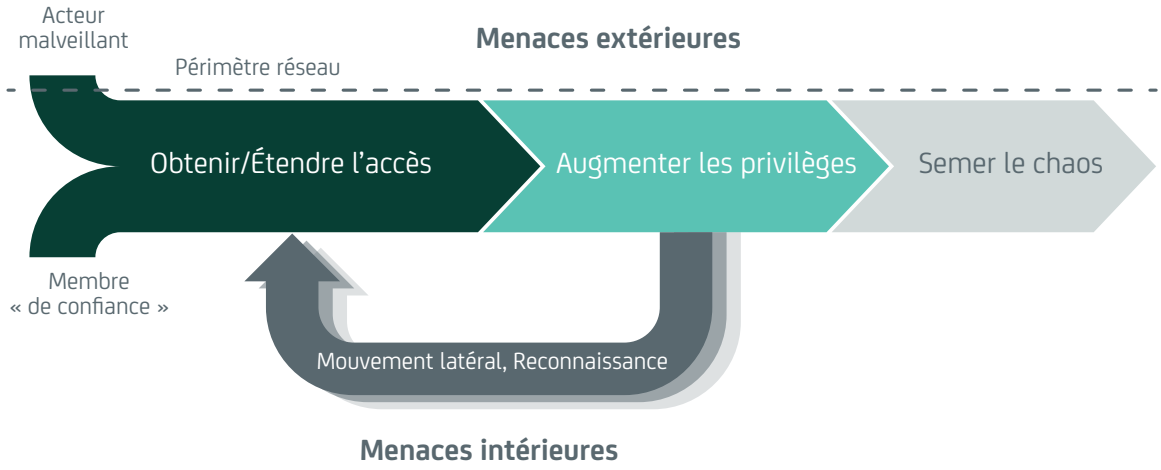
Dernier point, et peut-être le plus important, n'oublions pas que nous ne parlons pas là uniquement des utilisateurs à forts privilèges, mais plutôt de l'ensemble des données d'identification et des comptes à forts privilèges qui leurs sont associés et qui existent dans toute organisation standard. Ce sont ces données d'identification qui représentent la principale menace car leur exploitation est critique dans la mise en œuvre des attaques.

Présentation de la chaîne de frappe : pourquoi cela fonctionne

La chaîne de frappe d'une violation de sécurité se compose d'une série d'étapes immuables et prévisibles que le pirate informatique doit exécuter pour atteindre son objectif. Bien que la reconstitution de certaines chaînes de frappe puisse être complexe, il est possible de résumer simplement les étapes clés associées à une violation de données classique.

Illustration C.

Exemple de chaîne de frappe simplifiée.



Cette chaîne de frappe comprend quatre étapes clés :

- **Obtenir l'accès :** tout d'abord, il est nécessaire d'accéder au réseau. Si vous faites partie de l'organisation, en tant qu'utilisateur interne ou tiers autorisé, cette partie est facile ; il vous suffit d'utiliser les données d'identification et l'accès dont vous bénéficiez déjà. Toutefois, cela n'est pas beaucoup plus difficile pour un attaquant extérieur. La popularité grandissante des réseaux sociaux tels que LinkedIn permet d'identifier et de cibler assez facilement, au sein de l'organisation, les personnes disposant vraisemblablement d'un accès privilégié aux systèmes. Grâce à la sophistication croissante des techniques d'hameçonnage ciblé, il n'a jamais été aussi facile pour les pirates de duper même le plus expérimenté et le plus compétent des utilisateurs, et de le convaincre de fournir ses données d'identification, tout particulièrement celles relativement peu avancées comme les ID utilisateur et les mots de passe.
- **Augmenter les privilèges :** une fois que le pirate a accès au réseau, l'une de ses premières actions consiste à augmenter ses privilèges, généralement en compromettant d'autres identifiants à forts privilèges. Cette étape vient en soutien de deux activités essentielles. Premièrement, elle permet au pirate de prendre les mesures nécessaires pour que son existence et ses actions ne soient pas détectées, par exemple en altérant ou en désactivant la journalisation ou en installant des logiciels malveillants. Deuxièmement, elle prépare la voie pour la prochaine phase de la chaîne de frappe, à savoir la reconnaissance et le mouvement latéral.
- **Effectuer une reconnaissance et un mouvement latéral :** à moins d'être particulièrement chanceux, le premier système auquel le pirate a accès n'est généralement pas sa cible finale. Son objectif (les systèmes de traitement des cartes de paiement, les données propriétaire, les dossiers personnels, etc.) est probablement situé ailleurs sur le réseau, sur d'autres systèmes. La prochaine étape dans la chaîne de frappe est donc d'effectuer une reconnaissance du réseau et d'accéder à des systèmes et des serveurs plus proches de l'objectif final.
- **Répéter le processus au besoin :** à partir de là, c'est très simple, il suffit de répéter le processus jusqu'à atteindre l'objectif final, quel qu'il soit. À nouveau, l'expérience montre que les pirates peuvent être remarquablement patients, prenant le temps de naviguer dans les réseaux pour exécuter leur mission. Les rapports de violations indiquent régulièrement que le pirate avait pénétré le réseau de la victime depuis plusieurs mois, voire parfois plusieurs années. Une fois l'objectif final atteint, le pirate peut mener à bien son attaque, qu'il s'agisse de perturber les systèmes, de dérober des données ou autre.

Malheureusement, et tout particulièrement en l'absence d'outils et de processus de gestion des accès à forts privilèges, même des plus rudimentaires, la façon dont les entreprises opèrent facilite souvent le travail des pirates dans la mise en place de leur chaîne de frappe. Voici quelques-unes des erreurs les plus courantes :

- **Utilisation de techniques d'authentification faibles** pour l'accès au réseau ou à des ressources spécifiques, notamment la non-suppression des comptes et des mots de passe administrateur par défaut et l'utilisation de données d'identification peu sophistiquées, comme une simple combinaison ID utilisateur/mot de passe, facile à voler ou à compromettre.
- **Gestion des clés d'accès et des mots de passe insuffisante**, dans laquelle les données d'identification ne sont pas changées de manière fréquente et régulière. Dans les organisations comptant des milliers de collaborateurs, cela peut être extrêmement problématique, car il est tentant d'éviter les problèmes opérationnels et de réduire les coûts en mettant en place des pratiques de faible qualité, par exemple en réutilisant les identifiants ou en ne les changeant pas régulièrement.
- **Autoriser l'utilisation de comptes partagés**, tout particulièrement lorsqu'il s'agit de comptes à forts privilèges comme les comptes root ou administrateur. Cette pratique génère de multiples risques, car il est alors facile pour un utilisateur de partager ses données d'identification avec d'autres. Comme de nombreuses personnes ont accès aux mêmes identifiants, il est impossible de déterminer qui a effectué une tâche système particulière, ce qui complique les analyses et le dépannage.
- **Assimiler authentification et contrôle d'accès.** De nombreux réseaux ne sont pas correctement segmentés, ce qui a pour conséquence que tout individu ayant accès au réseau dispose d'une visibilité sur un grand nombre de ressources, bien plus qu'il n'est nécessaire ou prudent d'avoir. Ceci simplifie l'étape de reconnaissance et de mouvement latéral, permettant au pirate d'atteindre plus facilement son objectif final.
- **Absence de supervision et d'analyse de l'activité des utilisateurs à forts privilèges**, qui peut engendrer de nombreux problèmes. Sans supervision ni analyse régulière de l'activité, il est facile de ne pas remarquer un comportement suspect, permettant aux pirates d'agir en toute liberté. En outre, il est dans la nature humaine de faire des entorses au règlement, voire de ne pas le respecter, s'il y a peu de risques de se faire prendre.

Recommandations : rompre la chaîne de frappe

Divisée globalement en trois phases clés, la gestion des accès à forts privilèges offre différentes méthodes pour rompre la chaîne de frappe et empêcher les violations de sécurité.

Phase 1 : prévenir les accès non autorisés

Imposer aux utilisateurs à forts privilèges d'accéder aux ressources via une passerelle réseau est une façon simple d'appliquer une authentification robuste. Un tel système devrait bien entendu s'intégrer à toute infrastructure de gestion des identités existante. Le système doit donc supporter des liaisons vers les référentiels d'identités existants, de type Active Directory ou LDAP, voire même RADIUS ou TACACS+ dans certains environnements. Bien que le système puisse et doive supporter l'authentification locale, l'organisation dispose en général d'un référentiel d'identités bien en place. Étant donné que ces systèmes définissent déjà à la fois les utilisateurs autorisés et les rôles et autorisations, il est intéressant pour vous de mettre à profit ces données comme base pour les accès à forts privilèges.

Toutefois, ce n'est là qu'une simple base. Face à la simplicité relative avec laquelle les données d'identification des utilisateurs autorisés sont dérobées, une simple passerelle ne parviendra pas à bloquer un attaquant. Il est essentiel d'imposer l'utilisation d'une authentification multifacteur (MFA, Multi-Factor Authentication) pour les accès à forts privilèges. L'ajout d'une authentification MFA complique de manière significative la tâche de l'attaquant dans sa tentative d'accéder au réseau. Par le passé, ce type d'authentification faisait appel à une technologie coûteuse et très lourde d'un point de vue administratif. Toutefois, les progrès technologiques ont radicalement changé la mise en œuvre des

technologies d'authentification multifacteur et, au vu des risques élevés associés aux accès à forts privilèges, toute analyse coût/bénéfice, même rudimentaire, encouragera clairement son adoption.

L'utilisation d'une authentification multifacteur est également devenue aujourd'hui une problématique de mise en conformité et d'audit. Le gouvernement fédéral américain a très tôt pris des décisions dans ce sens, avec la création de normes imposant l'utilisation de cartes baptisées PIV/CAC pour l'accès administrateur aux systèmes. Les cartes PIV (Privileged Identity Verification, vérification des identités à forts privilèges) sont destinées aux organismes civils et les cartes CAC (Common Access Card, carte d'accès commun) sont utilisées pour les structures militaires. Ces cartes permettent l'identification des individus sur la base d'une infrastructure de clés publiques (PKI), en l'associant à une vérification d'identité, ce qui offre un degré de fiabilité élevé quant à l'identité de l'utilisateur. Des normes similaires ont également été intégrées à diverses obligations réglementaires, notamment dans le cadre de la récente révision de la norme PCI-DSS (Payment Card Industry Data Security Standard, norme de sécurité des données pour le secteur des cartes de paiement).

D'autres mesures qui tombent sous le coup du bon sens peuvent être utilisées pour minimiser les risques d'accès non autorisé, par exemple les restrictions d'accès aux systèmes en fonction de l'heure de la journée ou de l'adresse IP source de connexion de l'utilisateur. Ce type de contrôle peut être mis en place à la fois via une passerelle de gestion des accès à forts privilèges et par des contrôles basés sur agent, sur des ressources ou des serveurs spécifiques. Si un utilisateur donné se connecte habituellement durant une plage horaire spécifique ou depuis un endroit donné, il n'y aucune raison de lui octroyer un accès sans restriction. Vous pouvez choisir de bloquer complètement toutes les tentatives de connexion depuis une plage d'adresses, pour lesquelles toute demande d'accès semble étonnante, voire anormale.

Le deuxième aspect de ce problème est la protection des données d'identification utilisées pour accéder réellement aux systèmes gérés. Comme nous l'avons expliqué précédemment, il est malheureusement trop fréquent que ces identifiants soient insuffisamment protégés, partagés sans précaution ou mal gérés, ce qui présente des risques évidents pour la sécurité. Dans l'idéal, un système de gestion des accès à forts privilèges doit offrir un espace sécurisé pour le stockage chiffré des mots de passe et des paires de clés, à l'abri des regards indiscrets et des utilisateurs malveillants. Cet espace sécurisé doit avoir la capacité de gérer activement les données d'identification, en interagissant avec les systèmes pour modifier les mots de passe sur la base de normes adaptées au niveau de risques des ressources ou de l'organisation. L'automatisation de ce processus réduit à la fois les risques pour la sécurité (car il est alors possible de mettre à jour régulièrement les données d'identification de milliers, voire de centaines de milliers d'utilisateurs tout en conservant ces données dans un espace sécurisé) et les risques opérationnels, car l'automatisation de la mise à jour des mots de passe et des clés de sécurité est moins source d'erreurs. Associée à un processus d'authentification unique des utilisateurs à forts privilèges, cette solution peut offrir un degré de sécurité élevé car il est possible d'octroyer aux utilisateurs l'accès au système sans avoir à leur fournir concrètement des données d'identification pour ce faire. Et si un utilisateur ne possède pas de données d'identification, il ne peut pas les voler, les partager ou les transmettre de manière involontaire à un pirate.

Phase 2 : limiter l'escalade des privilèges, la reconnaissance et le mouvement latéral

Ceci offre une transition vers l'étape suivante dans la rupture de la chaîne de frappe, à savoir limiter la capacité d'un utilisateur à effectuer une reconnaissance du réseau et à s'y déplacer. Malheureusement, dans de nombreux réseaux, l'authentification finit toujours par ressembler à un simple contrôle d'accès : une fois connecté au réseau, vous avez fréquemment accès à l'ensemble des ressources. Pour un pirate, c'est évidemment une bonne nouvelle ! Il a le temps et souvent les moyens nécessaires pour naviguer de système en système, afin de se rapprocher de sa cible.

Les fonctionnalités telles que l'authentification unique des utilisateurs à forts privilèges aident à faire face à ces problèmes. L'approche est fondée sur un contrôle d'accès à privilèges minimaux, appelé contrôle d'accès « confiance zéro » (Zero Trust). Lorsque vous séparez l'authentification et l'accès au système de gestion des accès à forts privilèges de l'accès réel aux ressources gérées, les utilisateurs voient uniquement les systèmes et les ressources définis et autorisés dans votre règle de sécurité. Si les fonctions professionnelles d'un utilisateur donné exigent l'accès à un serveur ou une classe de ressources spécifique, il ne doit pas pouvoir accéder à d'autres parties du réseau. En appliquant des sessions de proxy ou de courtage entre le système de gestion des accès à forts privilèges et les ressources gérées, il est possible de limiter les droits qu'un utilisateur a sur un système et de contrôler les commandes qu'il peut émettre, ce qui réduit encore le risque qu'un utilisateur malveillant augmente ses privilèges ou se déplace latéralement au sein du réseau.

Par exemple, avec une session de proxy, il est possible de connecter un utilisateur à un système avec un compte standard, même s'il s'agit d'un utilisateur à forts privilèges comme un utilisateur root. Étant donné que le système peut appliquer des filtres de commande, il est possible de restreindre l'utilisateur à des commandes spécifiques ou de lui en interdire d'autres. Imaginons, par exemple, un utilisateur qui a pour tâche de mettre à jour un logiciel sur un ensemble de serveurs, tâche pour laquelle il peut être nécessaire de se connecter en tant qu'utilisateur root. Grâce aux filtres de commande, il est possible de connecter l'utilisateur et de lui autoriser uniquement les commandes nécessaires pour exécuter sa tâche. Toute autre commande, comme, par exemple, arrêter un processus ou redémarrer le système, lui sera interdite.

Des contrôles supplémentaires permettent de mettre en place des réponses variables en cas de tentative de violation des règles. Imaginons qu'un utilisateur émette une commande non autorisée ; les règles que vous avez établies peuvent supposer que cette action est le résultat d'un besoin réel ou d'une erreur innocente. Dans ce cas, un avertissement est envoyé à l'utilisateur et la commande est bloquée. Des tentatives répétées ou des infractions plus sérieuses peuvent mettre fin à la session, voire même désactiver le compte de l'utilisateur jusqu'à ce que l'administrateur puisse étudier en détail l'incident.

L'ajout d'agents basés sur un hôte offre des fonctionnalités similaires, mais avec des contrôles à la granularité plus fine, par exemple la possibilité de restreindre de manière stricte l'accès à des fichiers et des répertoires ou de superviser des fichiers pour modification. Il est également possible d'empêcher les tentatives de déplacement latéral au sein du réseau. Par exemple, après avoir obtenu l'accès à un système, un pirate peut tenter d'émettre une commande SSH ou TELNET ou bien d'ouvrir une session RDP distante vers le système ciblé. À nouveau, le système de gestion des accès à forts privilèges examine les règles de sécurité et détermine si cette activité est autorisée. Si ce n'est pas le cas, la commande est bloquée et la tentative de violation est consignée dans un journal.

Phase 3 : superviser, consigner et auditer l'activité

Idéalement, notre attaquant ne doit jamais parvenir à son objectif final ; les nombreux contrôles et vérifications définis et mis en place par le système de gestion des accès à forts privilèges offrent de multiples opportunités pour rompre la chaîne de frappe. La phase finale de supervision, de consignation et d'audit de l'activité est une mesure dissuasive supplémentaire contre les violations, mais elle offre également des avantages indéniables dans l'éventualité où la violation aurait tout de même lieu.

Comme nous l'avons fait remarquer, savoir que leur activité est consignée et analysée peut être extrêmement dissuasif pour les utilisateurs et les inciter à ne pas avoir de comportement malveillant, mais également à éviter toute activité d'exploration ou d'examen des systèmes qui, bien qu'apparemment innocente, serait potentiellement dangereuse. Les fonctionnalités étendues de journalisation, d'alerte, d'enregistrement et de reporting constituent un « système d'alerte précoce » qui prévient les autres administrateurs, responsables et auditeurs de tout comportement suspect ou inhabituel. Les alertes et les événements avertissent immédiatement de toute violation ou tentative de violation des règles de sécurité, ce qui permet de réagir rapidement. Les journaux peuvent ensuite être analysés, individuellement ou via un système de gestion des journaux ou SIEM, dans le contexte d'une autre activité système, afin de fournir plus d'informations sur les événements suspects, permettant d'enquêter avant que la violation ait lieu.

Étant donné que les comptes d'administrateur partagés sont couramment utilisés, la capacité à retracer les actions de chaque utilisateur de ces comptes est une priorité en termes d'exigences de conformité.

Enfin, l'enregistrement de session offre également de nombreux avantages. Les administrateurs peuvent parfois faire des erreurs. Les enregistrements de session sont alors utiles, car ils permettent d'examiner l'activité passée et de déterminer précisément les actions entreprises lors d'une interaction donnée. Cela peut accélérer le dépannage, notamment lorsqu'un problème est détecté au niveau d'un système. Si une mise à jour ou un changement de configuration a été effectué lors d'une session de travail précédente, il peut être long et difficile de déterminer avec précision ce qu'il s'est passé. Les enregistrements de session permettent de revenir facilement sur les tâches réalisées, accélérant la récupération. Ils peuvent également être utilisés à des fins de formation, en permettant d'illustrer facilement où une erreur a été commise et quelle est la procédure à privilégier.

Bien entendu, dans le pire des cas, c'est-à-dire en cas de violation de sécurité avérée, ces enregistrements et journaux peuvent être cruciaux pour déterminer exactement ce qu'a subi le système, quelles informations ont été prises et comment les ressources ont été compromises. Tout ceci accélère les analyses, aide à évaluer les dommages subis et fournit des informations précieuses pouvant être utilisées pour réduire les risques d'attaque future.

Avantages

Malheureusement, les violations de données, ainsi que les coûts et dommages qui en résultent, sont une réalité. Cependant, comme nous l'avons démontré dans ce document, les pirates suivent souvent un plan d'attaque établi et prévisible. La gestion des accès à forts privilèges offre de nombreux outils et contrôles qui agissent pour empêcher les pirates d'appliquer les étapes clés de leur plan d'attaque en rompant la chaîne de frappe. Elle contribue également à réduire les risques, à minimiser les dommages et à accélérer la récupération en cas de réussite de l'attaque. La mise en œuvre d'une solution complète de gestion des accès à forts privilèges offre les avantages suivants :

- **Réduction des risques.** Empêcher les accès non autorisés et limiter l'accès aux ressources une fois la connexion au réseau réussie. Protéger les mots de passe et autres données d'identification contre toute utilisation non autorisée et malveillante. Limiter les actions que les utilisateurs sont autorisés à réaliser sur les systèmes, prévenir l'exécution des commandes non autorisées et empêcher le mouvement latéral au sein du réseau.
- **Amélioration de la responsabilisation.** Retracer avec précision l'activité de chaque utilisateur, même en cas de compte partagé. Capturer l'activité et mettre en place des mesures dissuasives contre les comportements indésirables par le biais de fonctions complètes de journalisation, d'enregistrement de session et d'avertissements utilisateur.
- **Amélioration des audits et facilitation de la mise en conformité.** Simplifier la mise en conformité en supportant les exigences émergentes en matière d'authentification et de contrôle d'accès. Limiter la portée des exigences de conformité par le biais d'une segmentation logique du réseau.
- **Réduction de la complexité et amélioration de la productivité des opérateurs.** Limiter les risques, mais également améliorer la productivité individuelle des administrateurs en leur permettant d'accéder plus rapidement et plus facilement aux systèmes et aux ressources qu'ils doivent gérer grâce à l'authentification unique (SSO) des utilisateurs à forts privilèges. Simplifier la création et la mise en œuvre des contrôles de sécurité par le biais d'une définition et d'une application centralisées des règles de sécurité.

Conclusions

- Les données d'identification, les comptes et les identités à forts privilèges sont des ressources critiques pour les entreprises, qui doivent être protégées à tout prix en combinant technologies et processus via une gestion des accès privilégiés.
- Offrir une telle protection est essentiel pour rompre la chaîne de frappe des violations de données, et aide à prévenir les attaques et à minimiser l'impact si une telle attaque réussit.
- Un modèle de contrôle d'accès « confiance zéro » est essentiel pour tous les types d'accès à forts privilèges, qu'ils soient d'origine humaine ou automatique.
- Face aux failles des approches de sécurité par périmètre, une « défense en profondeur » est toujours la stratégie majeure pour la protection des ressources. La gestion des accès privilégiés est à même d'offrir plusieurs niveaux de défense supplémentaires autour des données d'identification, des comptes et des utilisateurs à forts privilèges, aussi bien au niveau des couches réseau que des hôtes.
- Face à la fréquence des attaques et à la sophistication des méthodes employées par les pirates, il est extrêmement tentant de se concentrer uniquement sur la détection et la réponse en cas de violations, et nos clients nous demandent souvent de le faire. C'est toutefois une erreur. Bien qu'il s'agisse là d'activités essentielles, il est crucial de rappeler que la gestion des accès à forts privilèges peut aider clairement les organisations à améliorer leur capacité de prévention de ces attaques.

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 solutions de gestion des accès à forts privilèges.

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 la performance 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 en savoir plus, rendez-vous sur **ca.com/fr**.

1 Intel Security et le Center for Strategic and International Studies, « Net Losses: Estimating the Global Loss of Cybercrime, Economic Impact of Cybercrime II », juin 2014, http://www.mcafee.com/fr/resources/reports/rp-economic-impact-cybercrime2.pdf

2 Forum économique mondial et McKinsey & Company, « Risk and Responsibility in a Hyper-connected World », janvier 2014, http://www3.weforum.org/docs/WEF_RiskResponsibility_HyperconnectedWorld_Report_2014.pdf

3 Eric M. Hutchins, Michael J. Cloppert, Rohan M. Amin, Ph.D., Lockheed Martin Corporation, « Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains », http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

4 Andras Cser, enquête Forrester Research, « Critical Questions to Ask Your Privileged Identity Management Solution Provider », 10 septembre 2014.

5 Ars Technica, « AWS console breach leads to demise of service with 'proven' backup plan », 18 juin 2014, http://arstechnica.com/security/2014/06/aws-console-breach-leads-to-demise-of-service-with-proven-backup-plan/

6 Brian Krebs, « China To Blame in Anthem Hack? », 15 février 2015, http://krebsonsecurity.com/2015/02/china-to-blame-in-anthem-hack/

7 Anmol Singh et Felix Gaehtgens, « Twelve Best Practices for Privileged Access Management, Gartner », 8 octobre 2015, G00277332

CS200-162063_1115