**LIVRE BLANC** | OCTOBRE 2014

# Menaces persistantes avancées : se défendre de l'intérieur

Russel Miller
CA Technologies, Gestion de la sécurité

ca technologies

# Table des matières

# Résumé


## Défi

Assurer la sécurité d'une organisation est un défi de plus en plus difficile. Les attaques toujours plus complexes et l'augmentation des APT (Advanced Persistent Threats), un type d'attaque ciblée, ont fait prendre conscience aux organisations de leur vulnérabilité en cas d'attaque. Des sociétés telles que RSA Security, Google et Northrop Grumman ont découvert qu'elles étaient la cible d'APT. Ne pas avoir été victime d'une faille grave par le passé ne garantit aucunement la sécurité future. Les organisations spécifiquement ciblées par une APT font face à des défis inhabituels pour les administrateurs de sécurité, par exemple l'étalement des actions sur plusieurs mois ou années pour éviter toute détection. L'impact des failles est également toujours plus important ; c'est là un véritable défi pour les dirigeants.

## Solution

Il n'y a pas de « remède miracle » pour se défendre contre les APT. Plusieurs couches de protection doivent être combinées pour réduire à la fois le risque de faille et pour atténuer l'impact en cas de faille.

L'approche initiale de défense contre les attaques ciblées reposait sur la sécurisation du périmètre à l'aide de pare-feu et de systèmes de détection des instructions, permettant de déceler et de bloquer tout comportement anormal. Cette approche peut être efficace contre certains types d'attaques, mais non contre tous les types de vecteurs d'attaque, tels que le « spear phishing » (attaques avec phishing dirigé) et « l'ingénierie sociale ».

Si aucun produit de sécurité (technologique ou autre) ne peut totalement protéger une organisation contre les APT, les solutions de sécurité interdomaines actuelles peuvent aider les organisations à se protéger mieux que jamais. Fonctionnant généralement en silos, la gestion des identités à privilèges, le contrôle et la protection des informations et la sécurité de l'infrastructure interne peuvent désormais être combinés pour permettre aux organisations d'assurer la sécurité de leur infrastructure informatique et de leurs data centers, de façon complémentaire. CA Technologies parle d'intelligence d'identité et de données.

## Avantages

C'est en analysant les APT et en se protégeant que les organisations peuvent réduire les risques si elles sont la cible spécifique d'une attaque. Ces risques peuvent être d'ordre financier, mais également concerner la réputation, la bonne marche des opérations, ainsi que les aspects juridiques et réglementaires.

Si la sécurité déployable contre les APT est considérée sous un angle holistique, l'organisation se protège du même coup contre les attaques automatisées, moins sophistiquées, y compris internes. Une approche globale de la sécurité présente bien d'autres avantages, comme l'amélioration de la conformité, la possibilité d'adopter des services Cloud, le renforcement de la sécurité de la virtualisation et la réduction des coûts.

**Section 1 : Défi**

# Menaces persistantes avancées : bien loin de la routine

Les menaces persistantes avancées posent des défis distincts des risques de sécurité classiques. Une menace persistante avancée est une attaque sophistiquée à long terme d'une entité spécifiquement ciblée. Souvent, l'attaquant est commandité par un État, visant à tirer profit d'informations de la plus haute importance d'autres gouvernements. Cependant, une organisation privée peut également être la source ou la cible d'une attaque. Ce terme a été utilisé pour la première fois par l'armée de l'air des États-Unis en 2006.[1] Le National Institute of Standards and Technology (NIST) définit les menaces persistantes avancées (APT) comme suit :[2]

« Une menace persistante avancée est un adversaire disposant d'un niveau sophistiqué d'expertise et de ressources significatives qui lui permettent, grâce à plusieurs vecteurs d'attaque (par ex. cybernétique, physique ou tromperie), de créer les conditions requises à la réalisation de ses objectifs, lesquels consistent généralement à créer et développer une brèche au niveau de l'infrastructure IT des organisations. Le but de cet attaquant est l'exfiltration continue d'informations et/ou le sabotage ou le blocage d'aspects critiques d'une mission, d'un programme ou d'une organisation, ou son positionnement stratégique en ce sens pour une action ultérieure de ce type. En outre, une menace persistante avancée poursuit des objectifs sur une période prolongée, s'adaptant aux efforts de défense de la partie attaquée, avec une détermination sans faille pour maintenir le niveau d'interaction nécessaire à la réalisation de ses objectifs. »

Il existe d'autres définitions d'une menace persistante avancée, la plus claire étant celle tenant compte du sens de chacun des trois mots.[3]

- **Menace :** pour qu'il y ait menace, l'attaquant doit disposer à la fois de la motivation et de la capacité à mener à bien une attaque.
- **Persistante :** les APT s'étendent souvent sur une longue période. Contrairement aux attaques à court terme profitant d'opportunités temporaires, les APT peuvent s'étendre sur plusieurs années. Plusieurs vecteurs peuvent être utilisés, allant des attaques Internet à l'ingénierie sociale. Des failles de sécurité mineures peuvent être combinées au fil du temps pour accéder à des données bien plus sensibles.
- **Avancée :** l'attaquant dispose des capacités techniques suffisantes pour exploiter les vulnérabilités au niveau de la cible. Cela peut inclure l'accès à d'importantes bases de données de vulnérabilités et des compétences de codage, mais également la capacité à découvrir et à utiliser des vulnérabilités jusque-là inconnues.

Les outils totalement automatisés ne sont pas identifiés comme APT à part entière bien qu'ils puissent être utilisés par un groupe organisé et coordonné dans le cadre d'une attaque de grande envergure.

## Étapes

Une menace persistante classique se compose des quatre étapes suivantes :

**Illustration A.**

Quatre étapes d'une menace persistante avancée


1. **Reconnaissance :** enquête sur les vulnérabilités d'une organisation. Cela inclut une recherche basique, notamment des requêtes de domaine, mais aussi des analyses portant sur les ports et les vulnérabilités.
2. **Entrée initiale :** exploitation d'une faiblesse pour ouvrir une brèche dans le réseau cible. Ceci peut être effectué grâce à des méthodes techniques sophistiquées ou des techniques telles que le « spear phishing » (attaques avec phishing dirigé), permettant un accès régulier à un système unique. « L'ingénierie sociale », ou exploitation des personnes, constitue également une méthode courante d'accès.
3. **Élévation de privilèges et expansion du contrôle :** lorsque l'attaquant pénètre dans le périmètre réseau, il tente d'acquérir des privilèges et un contrôle accrus sur des systèmes critiques. Cette étape peut également impliquer l'installation d'outils de type « porte dérobée » pour simplifier les prochains accès au réseau.
4. **Exploitation continue :** une fois le contrôle établi, l'attaquant peut exporter des données sensibles de façon continue.

Les troisième et quatrième étapes peuvent se dérouler sur plusieurs années, pour réduire le risque de détection.

## En quoi les APT sont-elles différentes ?

La différence la plus critique entre les APT et les menaces « normales » réside dans le fait qu'une organisation est ciblée de manière spécifique. Si la défense du « périmètre » et des contrôles de sécurité classiques peuvent protéger une organisation contre des attaques standard, ces techniques peuvent s'avérer insuffisantes contre les APT. Les attaquants les plus patients attendent que de nouvelles vulnérabilités ouvrent une brèche ou que des vulnérabilités apparemment moins importantes se combinent pour générer une attaque de grande échelle, dévastatrice.

Dans le cas d'une telle menace, les règles normales ne s'appliquent pas. Auparavant, de nombreuses organisations avaient simplement besoin d'un niveau de sécurité supérieur à celui des autres organisations et entreprises connectées à Internet, dans la mesure où bon nombre d'attaquants choisissaient les cibles plus faciles. Toutefois, à cause de ces APT, les organisations doivent être en mesure de faire échouer un ennemi motivé qui prend suffisamment de temps pour examiner les failles au lieu de s'attaquer à une autre cible.

La durée des APT peut également rendre leur détection particulièrement complexe. En cas de faille de sécurité standard, un volume important de données peut être exporté en peu de temps, ce qui permet de découvrir la faille par le biais du pare-feu et de périphériques de détection des intrusions. Dans le cadre d'une APT, un attaquant peut mettre des mois, voire des années, pour exporter les données ciblées, contournant même les systèmes disposant de toutes les options de sécurité possibles.

| Objectifs | Cibles |
|---|---|
| Du fait de leur nature ciblée, les APT ont souvent des objectifs différents de ceux des pirates Internet traditionnels, notamment un intérêt particulier pour les points suivants, et non pour un simple vol ou des dégâts d'amateurs :<br>▪ Manipulation politique<br>▪ Espionnage militaire<br>▪ Espionnage financier<br>▪ Espionnage industriel<br>▪ Extorsion financière | Certains types précis d'organisations sont plus sujets aux APT car la menace est souvent liée à un financement étatique ou politique :<br>▪ Agences gouvernementales<br>▪ Organisations et sous-traitants du secteur de la défense<br>▪ Systèmes d'infrastructures critiques (p. ex., services publics, moyens de communication et de transport)<br>▪ Organisations politiques<br>▪ Institutions financières<br>▪ Entreprises technologiques |

## Exemples

### RSA

En 2011, RSA Security a déclaré avoir été victime d'une APT[4]. Les attaquants ont obtenu l'entrée initiale en trompant un utilisateur interne afin qu'il ouvre un courriel avec en pièce jointe une feuille de calcul exploitant une vulnérabilité « jour zéro » dans Adobe Flash. À partir de là, ils ont augmenté leurs privilèges, installé des portes dérobées et pris le contrôle d'autres systèmes.

Les attaquants ont alors été en mesure d'accéder aux systèmes RSA hébergeant des informations liées à leurs jetons d'authentification à deux facteurs ou SecurID. Ces informations pouvaient inclure des valeurs « de départ », utilisées par RSA avec des jetons pour générer des mots de passe temporaires, changeant toutes les 60 secondes. Si le code source lui-même était volé, les attaquants pouvaient chercher des vulnérabilités dans le déploiement SecurID ou dans le chiffrement.

### Opération Aurora

Opération Aurora est une APT qui a ciblé de nombreuses multinationales, telles que Google, Adobe, Rackspace et Juniper Networks. La presse a révélé que de nombreuses autres sociétés auraient été ciblées, notamment Yahoo, Northrop Grumman, Morgan Stanley, Symantec et Dow Chemical.[5] Le Politburo chinois aurait dirigé les attaques dans le cadre d'une campagne de grande envergure contre les États-Unis et d'autres pays occidentaux.[6]

**Section 2 : Solution**

# Défense approfondie

L'élément clé pour se défendre contre les APT est une défense approfondie. Avec suffisamment de temps, un attaquant déterminé peut ouvrir une faille dans la plupart des périmètres réseau. Une stratégie de défense efficace permet de remplir les objectifs suivants :

1. Entraver l'accès initial.
2. Réduire le risque d'élévation de privilèges en cas de compte compromis.
3. Limiter l'impact potentiel lié à un compte compromis, même s'il s'agit d'un compte à forts privilèges.
4. Détecter les comptes compromis et toute activité suspecte de façon anticipée dans le processus.
5. Recueillir des informations pratiques dans le cadre d'une enquête, afin de pouvoir identifier les dommages, le moment où ils sont survenus et leur auteur.

Assurer la sûreté du périmètre grâce à des pare-feu et des systèmes de détection des intrusions aux frontières du réseau n'est efficace que pour les points 1 et 4. Il est donc nécessaire de mettre en place une stratégie de protection plus active.

## Détection anticipée

Souvent, les failles sont détectées après que l'attaquant a réussi à accéder au réseau interne et provoqué des dégâts ou volé des volumes importants de données. À ce stade, la « défense » contre les APT implique un processus coûteux de contrôle, de nettoyage et de supervision continue des dommages. La clé d'une protection abordable et gérable contre les APT consiste à détecter les menaces aussi tôt que possible. Durant la phase initiale d'une attaque, lorsque l'attaquant met un pied dans le réseau, l'organisation peut utiliser diverses techniques pour détecter la faille, y compris la séparation et l'externalisation de la sécurité système par rapport à l'administration système, la prévention et la détection des tentatives d'élévation de privilèges et de l'utilisation de privilèges non autorisée, ainsi que l'audit et l'enregistrement de l'activité des utilisateurs en dehors des journaux du système d'exploitation (l'audit et l'enregistrement peuvent se faire par exemple à l'insu de l'attaquant).

Outre la détection précoce des failles, la gestion des identités à forts privilèges, le contrôle et la protection des informations, ainsi que la sécurité de l'infrastructure interne constituent le cœur d'une défense approfondie contre les APT. Ces techniques sont détaillées dans les sections suivantes.

## Gestion des identités à forts privilèges

Les outils PIM (Privileged Identity Management, gestion des identités à forts privilèges) gèrent et supervisent les comptes d'administration, tels que le compte « Administrateur » sous Windows et « root » pour UNIX et Linux. Les systèmes PIM :

- Implémentent le principe des « privilèges minimaux », même pour les comptes d'administration.
- Gèrent l'accès aux comptes partagés via des fonctionnalités de gestion des mots de passe des utilisateurs à forts privilèges.
- Suivent les activités des utilisateurs, tant pour assurer la responsabilisation que pour faciliter les enquêtes en cas de failles de sécurité.

## Privilèges d'accès minimaux

Toute personne doit disposer du minimum de privilèges nécessaires à son travail. Même si la plupart des organisations ont compris ce principe, elles peinent souvent à l'appliquer dans la pratique, en particulier pour les comptes d'administration. Les individus ayant besoin d'un certain type d'accès privilégié se voient généralement remettre le mot de passe du compte d'administration pertinent, partagé par plusieurs personnes.

Les organisations doivent réaliser qu'avec la prédominance croissante des APT, un accès privilégié n'est pas forcément de type « tout ou rien ». Il est possible d'attribuer des privilèges élevés à des individus uniquement pour qu'ils puissent accomplir une seule tâche bien spécifique. Auparavant, sur les systèmes UNIX et Linux, l'outil « sudo » était utilisé à cet effet, mais les outils de contrôle d'accès actuels permettent d'autoriser et d'interdire un accès de façon centralisée, à la fois pour les systèmes UNIX et Windows®.

## Modèle de sécurité : séparer la sécurité de l'administration système

Généralement, un système d'exploitation utilise un modèle de sécurité bicouche : utilisateurs à forts privilèges et utilisateurs ordinaires. Toutefois, pour une protection efficace contre les APT, un modèle plus sophistiqué est requis. Ce modèle repose sur les principes de sécurité standard des « privilèges minimaux » et de la « séparation des fonctions ». Au moins trois rôles d'administration principaux doivent être définis :

- **Administrateur système :** l'administrateur du système doit disposer des privilèges nécessaires pour mettre à jour les logiciels de serveur, modifier les paramètres de configuration et installer des logiciels. Par contre, les administrateurs système ne doivent pas être en mesure de modifier des paramètres de sécurité critiques ou de consulter les journaux liés à la sécurité.
- **Administrateur de sécurité :** ces administrateurs doivent pouvoir mettre à jour et modifier les paramètres de sécurité et les configurations, mais aussi consulter les fichiers journaux liés à la sécurité. En revanche, ils ne doivent pas pouvoir installer des logiciels ou accéder à des données sensibles sur un système.
- **Auditeur :** les auditeurs doivent avoir la possibilité de vérifier les paramètres de sécurité et de consulter les fichiers journaux, sans pouvoir apporter de modifications à un système. Si l'accès aux fichiers sensibles peut être autorisé, tous les accès doivent être en lecture seule.

D'autres types d'administrateurs peuvent être créés si nécessaire, par exemple des administrateurs de base de données ou de toute autre application particulièrement sensible.

L'utilisation d'un modèle de sécurité multiniveau répond à deux objectifs à la fois : ce type d'approche offre une protection contre les menaces internes (administrateurs internes), en limitant les opérations que chaque individu peut effectuer, et complique les tentatives d'APT des attaquants externes. Au lieu de devoir s'attaquer à un compte « superutilisateur », les attaquants doivent maintenant réussir à accéder à plusieurs comptes pour disposer d'un accès total au système.

## Contrôles affinés

Des contrôles affinés, en plus d'être une bonne pratique de sécurité, sont particulièrement utiles pour atténuer l'impact d'une APT. Une fois que les attaquants ont acquis des privilèges d'administration, ils installent généralement des « rootkits » de type porte dérobée et commencent à exporter des données sensibles. Avec des contrôles d'accès adaptés, l'attaquant, même doté de privilèges, voit son champ d'action limité et peut être empêché d'accéder aux fichiers sensibles, d'exécuter des commandes malveillantes, d'installer des programmes, d'arrêter/de démarrer des services ou de modifier des fichiers journaux. Dans le cas d'un système avec contrôles affinés, l'attaquant peut être contraint de compromettre plusieurs comptes pour réaliser des opérations qui pouvaient auparavant être effectuées à l'aide d'un seul compte.

L'implémentation de contrôles d'accès affinés peut également atténuer la pire faiblesse d'une organisation : ses membres. Avec les techniques « d'ingénierie sociale », les attaquants peuvent tromper les employés et d'autres collaborateurs internes en leur faisant fournir des informations permettant d'accéder à leur compte ou de révéler d'autres failles de sécurité. En limitant l'accès aux systèmes critiques et aux données des employés, les dégâts que l'attaquant peut faire en accédant aux comptes par le biais de l'ingénierie sociale sont réduits.

## Gestion des comptes partagés

La gestion des comptes partagés (ou « gestion des mots de passe des utilisateurs à forts privilèges ») est l'une des clés de la protection contre les APT. Réussir à accéder aux identités à forts privilèges, souvent par le biais d'une élévation de privilèges, est l'une des étapes intermédiaires clés de la plupart des attaques menées à bien. Les outils de gestion des mots de passe utilisateur doivent remplir les objectifs suivants :

- Stocker de façon sécurisée les mots de passe chiffrés.
- Gérer la complexité des mots de passe et les changements automatiques, selon la règle.
- Limiter l'accès aux comptes d'administration, en exigeant que tous les accès passent par un portail centralisé.
- Utiliser la fonctionnalité de « connexion automatique » pour empêcher même les utilisateurs autorisés de connaître les mots de passe des comptes à forts privilèges.
- Octroyer un accès d'urgence à un compte, avec des contrôles supplémentaires et les approbations requises.
- Éliminer l'utilisation des mots de passe codés en dur dans les scripts, souvent stockés en texte clair et faciles à voler par un utilisateur malveillant.

Ces fonctionnalités empêchent non seulement le partage des mots de passe, mais aussi le vol de mots de passe à partir des fichiers de mots de passe personnels ou via des enregistreurs de frappe. En exigeant que toutes les connexions à des comptes à forts privilèges passent par un proxy central, l'organisation peut suivre toutes les connexions et activités en cas de faille, ce qui facilite les opérations d'investigation et réduit potentiellement les dégâts.

## Reporting de l'activité des utilisateurs

Le suivi des activités des comptes à forts privilèges est essentiel pour détecter les APT et atténuer leur impact en cas d'attaque initiale réussie. Par nature, les APT impliquent généralement l'exportation de volumes importants de données, susceptibles d'être détectés par les outils adéquats. Les journaux des activités des utilisateurs indiquent quelles activités système et utilisateur ont lieu sur un système ou un périphérique réseau, et peuvent être utilisés pour identifier les violations de règles et enquêter sur les failles de sécurité.

Des réglementations telles que HIPAA, CA SB 1386 et les nombreuses lois de notification de faille locales exigent que l'organisation fasse état de toute faille de sécurité à la personne ou à l'organisation concernée. Les journaux des activités des utilisateurs peuvent être utilisés pour enquêter sur une faille de sécurité et découvrir qui a fait quoi, mais aussi pour connaître les circonstances afin de rectifier les contrôles internes et d'améliorer les processus.

Les outils de reporting de l'activité des utilisateurs sont censés offrir les fonctionnalités suivantes.

- Suivi :
  - De toutes les connexions, en particulier pour les comptes partagés et à forts privilèges, y compris l'IP source, l'ID utilisateur d'origine accédant à un compte partagé, l'heure et la date de connexion et de déconnexion
  - De toutes les activités d'un compte partagé, jusqu'à l'ID utilisateur d'origine
  - De toutes les commandes, qu'elles aient été saisies depuis une ligne de commande ou une interface utilisateur graphique

- Détection de tout comportement anormal :
    - Identification des activités suspectes et déclenchement d'alertes
    - Corrélation des journaux, avec identification de l'individu ayant effectué une action spécifique via l'analyse de structures complexes et de journaux d'audit
- Étude des failles :
    - Possibilité de déterminer « qui a fait quoi » dans un environnement de comptes partagés
    - Mise à disposition d'outils visuels d'analyse de journaux dotés de fonctionnalités d'exploration approfondie permettant d'accélérer l'enquête sur les activités des utilisateurs et des ressources, ainsi que l'identification des violations de règles

En cas de faille, ces fonctionnalités peuvent aider l'organisation à comprendre les éléments suivants :

- Comment l'attaquant a réussi à accéder à un compte
- Ce qu'il a fait avec ce compte et quels sont les dégâts
- Comment empêcher les futures attaques à l'aide de méthodes identiques ou similaires
- Qui est l'attaquant et d'où vient-il
- Quelles sont les informations à communiquer aux autorités de contrôle

Il est essentiel de garder à l'esprit que les journaux doivent également être protégés contre les administrateurs. Les utilisateurs à forts privilèges peuvent déterminer où sont stockés les journaux en local sur les systèmes et découvrir les règles d'audit utilisées au sein de l'organisation. Ils peuvent effacer leurs propres traces en supprimant des entrées dans les fichiers journaux locaux grâce à leur accès complet aux systèmes (en l'absence de contrôles affinés adaptés). Les organisations doivent conserver les journaux à un emplacement distant inaccessible pour les utilisateurs à forts privilèges, et suivre toute tentative potentielle de suppression de fichiers journaux locaux sur les systèmes.

## Protection et contrôle des informations

Le but ultime d'une APT est le vol d'informations sensibles. Dès lors, le contrôle des données est un élément essentiel pour une protection efficace. Pour protéger les données sensibles contre les APT, l'organisation doit protéger et contrôler les données dans quatre états :

- **Données en cours d'accès :** tentative d'accès à des informations sensibles par un rôle non adapté
- **Données en cours d'utilisation :** informations sensibles en cours d'utilisation sur le poste de travail ou l'ordinateur portable local
- **Données en mouvement :** informations sensibles communiquées sur le réseau
- **Données au repos** : informations sensibles stockées dans des référentiels de type bases de données, serveurs de fichiers ou systèmes collaboratifs

Pour ce faire, les organisations doivent définir des règles permettant d'appliquer certaines méthodes de contrôle si un accès ou un usage non approprié des données est détecté. Lorsqu'une violation de règle survient (par exemple en cas de tentative d'accès à des informations sous propriété intellectuelle, de copie de ces données sur un lecteur USB ou de tentative d'envoi de ces informations par courriel), la solution utilisée doit limiter le préjudice tout en déclenchant une alerte.

La classification des informations est au cœur de toute initiative de protection des données. Sans connaître la nature des informations ni leur emplacement, il est impossible de déployer un programme de protection des données adapté. L'organisation doit détecter avec précision les données sensibles et les classer en fonction de leur niveau de sensibilité pour l'organisation. Ces données incluent la propriété intellectuelle, mais aussi les informations d'identification personnelle, informations médicales privées et autres informations non publiques.

Une fois les informations correctement classées, les règles définies et les contrôles déployés, l'organisation peut superviser et contrôler l'accès, ainsi que gérer toutes les informations sensibles. Cela inclut les actions utilisateur, depuis la simple tentative d'accès et de lecture des données sensibles, jusqu'à la copie sur un périphérique amovible, en passant par l'impression, l'envoi par courriel hors du réseau, ou encore la détection de données stockées dans un référentiel de type SharePoint.

## Sécurité de l'infrastructure interne

S'il est essentiel d'assurer la sécurité du périmètre réseau, des identités à forts privilèges et des données, il est également important d'assurer celle de l'infrastructure informatique interne pour bénéficier d'une protection approfondie contre les APT. Outre une architecture et une segmentation réseau adaptées, cela inclut une configuration et une sécurisation appropriées des serveurs et des périphériques individuels, ainsi que de leur environnement.

## Sécurité atypique et externalisée

Les attaquants élaborent des stratégies et utilisent des méthodes tactiques contre les dispositifs de sécurité connus. Ils utilisent également des commandes, des fonctions et des utilitaires de système d'exploitation courants pour recueillir des informations, superviser le système et passer à l'action afin d'étendre leur contrôle. Les professionnels de la sécurité peuvent utiliser les méthodes classiques des attaquants contre eux en ajoutant des éléments inattendus au système. Par exemple, des fichiers et des commandes qui ne semblent pas protégés ou supervisés par les journaux système peuvent l'être par un outil externe. En effet, les autorisations visibles par l'attaquant ne sont pas nécessairement celles réellement appliquées. Cela permet à l'organisation de détecter un attaquant en train de vérifier les autorisations d'un système d'exploitation et d'enfreindre les règles externes lorsqu'il teste les limites des autorisations.

C'est la principale raison pour laquelle l'administration de la sécurité doit être externalisée et séparée de l'administration du système d'exploitation. Généralement, après avoir réussi à accéder au système, l'attaquant tente d'élever ses privilèges afin de contourner les contrôles du système d'exploitation. Avec cet accès, il pense pouvoir contourner les mécanismes de sécurité et « effacer ses traces » efficacement. Avec une fonction de sécurité externe, il est souvent possible de détecter et de bloquer l'attaquant bien plus tôt dans le processus d'APT, lorsqu'il tente d'élever ses privilèges, de modifier des contrôles de sécurité des systèmes ou d'utiliser des privilèges qui ne lui ont pas été attribués. Bien que l'attaquant puisse réussir à contourner les contrôles classiques et les journaux au niveau du système d'exploitation, les processus de détection externes peuvent le déceler à son insu. Pour résumer, l'organisation peut déployer une règle de contrôle d'accès en arrière-plan, de façon puissante et inattendue.

En outre, les commandes système standard peuvent être modifiées ou remplacées. Si les administrateurs renomment des fonctions telles que « sudo », toutes les tentatives d'utilisation de la commande sudo d'origine peuvent déclencher une alerte et permettre la détection anticipée d'une faille.

## Renforcement des serveurs

Tous les serveurs hébergeant des informations sensibles doivent être configurés de manière à limiter les risques de compromission et, le cas échéant, de dissémination des données. Pour ce faire, les organisations doivent veiller à :

- Utiliser un pare-feu logiciel pour contrôler à la fois les communications entrantes et sortantes, limiter les paquets par IP source, protocole (p. ex., SSH, TELNET, etc.) et port TCP, bloquer les protocoles non sûrs (p. ex., les services non chiffrés comme FTP)
- Bloquer toutes les exécutions et installations d'applications, sauf en cas d'autorisation explicite (« liste blanche d'applications »), les exploits d'exécution de code et l'installation de tout logiciel type « porte dérobée »
- « Confiner » les applications. Définir et autoriser des actions permises pour les applications à haut risque et restreindre tout comportement dépassant ces limites. Par exemple, une liste de contrôle d'accès peut être créée en se basant sur un ID logique qui détient des processus et des services Oracle® afin que son confinement lui permette uniquement de démarrer les services de système de gestion de bases de données (DBMS) Oracle.
- Empêcher toute modification des fichiers journaux
- Superviser l'intégrité des fichiers pour détecter toute modification des fichiers clés, comme celles effectuées par les « rootkits »
- Contrôler l'accès aux fichiers de répertoires d'applications sensibles (p. ex. seule l'application de paie peut ouvrir les fichiers de paie)
- Détecter les modifications des fichiers sensibles en temps réel

## Sécurité uniforme

Les environnements informatiques distribués présentent un problème récurrent : la diversité des fonctionnalités et des disponibilités des contrôles de sécurité entre les plates-formes. Par exemple, les contrôles sur les répertoires/fichiers UNIX sont très différents de ceux sous Windows. Ceci peut mener à plusieurs problèmes exploitables :

- Règles de sécurité adaptées à un modèle de système plutôt qu'à un modèle de sécurité métier
- Règles de sécurité devant s'adapter aux contraintes des systèmes
- Erreurs et omissions dues à la complexité accrue de la gestion de la sécurité

Pour assurer une protection complète contre les APT, les configurations de sécurité doivent être appliquées de façon aussi homogène que possible à toutes les plates-formes. Toute limitation ou incohérence doit être comprise et suivie.

Une raison de plus pour que les organisations ne comptent pas que sur la sécurité du système d'exploitation. Les outils externes peuvent offrir une plate-forme universelle, permettant d'appliquer un paradigme de sécurité dans les divers environnements, pour une approche de la sécurité propre à l'activité métier, centralisée et rationalisée.

## Sécurité de la virtualisation

Le nombre de systèmes virtualisés a explosé, faisant des environnements virtuels une cible clé des attaquants opérant par APT. L'hyperviseur constitue également une cible critique du fait du niveau d'accès qu'il peut offrir. Si l'attaquant compromet l'hyperviseur, il peut pratiquement avoir accès à toutes les machines virtuelles exécutées sur cet hyperviseur. Bien que la sécurité au niveau du système d'exploitation puisse empêcher les connexions directes et que le chiffrement puisse protéger les données sensibles, ces mesures ne résisteront pas à un attaquant déterminé. Toute personne disposant d'un contrôle d'administration sur un hyperviseur peut copier des machines virtuelles complètes

dans un environnement externe, ainsi que contourner la sécurité basée sur les hôtes en utilisant des méthodes en force ou en remplaçant des fichiers clés.

Pour assurer la sécurité des environnements virtuels, les organisations doivent se concentrer sur les administrateurs et appliquer le principe des privilèges minimaux. D'abord, l'accès aux comptes d'hyperviseur à forts privilèges doit être strictement contrôlé, et toutes les actions doivent être supervisées et consignées. Ensuite, exactement comme pour les environnements physiques, les identités d'hyperviseur à forts privilèges doivent être autorisées à n'effectuer que les actions requises. Par exemple, les administrateurs financiers ne doivent pouvoir accéder qu'aux machines virtuelles du département Finances et non aux systèmes des RH.

## Rassembler pour mieux défendre

Il ne suffit pas d'un seul outil de sécurité pour défendre une organisation contre une APT menée par un attaquant bien informé, déterminé, compétent et tenace. Toute stratégie de défense contre les APT a pour but d'entraver autant que possible l'accès au réseau, de limiter l'impact potentiel et le volume d'informations volé en cas de faille, et de détecter celle-ci le plus rapidement possible.

Bien qu'un périmètre de sécurité soit un composant requis pour prévenir la faille initiale, il n'est nullement suffisant et s'avère inefficace une fois la faille ouverte. La clé pour atténuer les risques est une combinaison intelligente de gestion des identités à forts privilèges, de classification et de contrôle des données, et de sécurité de l'infrastructure.

Les outils standard de gestion des identités à forts privilèges peuvent limiter ou autoriser les accès sur la base d'un ensemble de règles. Ceci peut offrir une séparation pertinente des fonctions, mais il s'agit d'une solution rigide par nature. Les privilèges peuvent être modifiés par la suite pour les adapter aux rôles, mais cela n'est finalement qu'une solution passive.

C'est la « prise en compte du contenu » qui est requise pour passer à une nouvelle génération de défense active contre les APT. Cela revient à intégrer l'intelligence de données à chaque décision d'approbation ou de refus d'une demande d'accès. Pour ce faire, il faut reconnaître et comprendre les structures d'accès aux données et leur utilisation. Par exemple, les événements suivants doivent être pris en compte :

- **Modifications du type de données souhaité :** un administrateur accède toujours à un certain type de données (p. ex., des données de fonctionnement), puis demande l'accès à des données financières ou des données client confidentielles.
- **Modifications d'utilisation des données :** un administrateur accède généralement aux données sensibles par le biais d'une application précise, avec accès en lecture seule, puis demande à exporter des données sur un disque dur externe, un lecteur USB ou par courriel.
- **Modifications du volume de données :** un administrateur accède à 100 Mo de données par semaine, puis demande à accéder à 500 Go pour la même période.
- **Modifications de la fréquence d'accès aux données :** un administrateur accède à des données hautement confidentielles une fois par mois, puis souhaite soudainement y accéder quotidiennement.

Aucune de ces modifications n'est en soi révélatrice d'une faille ; toutefois, elles représentent des changements de comportement. Tout système contrôlant de façon intelligente les accès des utilisateurs à forts privilèges doit tenir compte de ces facteurs lorsqu'il examine une demande d'accès. Cette intelligence de données peut être utilisée pour refuser l'accès à des ressources en temps réel ou autoriser l'accès tout en créant une alerte signalant une activité suspecte.

**Section 3 : Avantages**

## Réduisez les risques

Les organisations ciblées par une APT font face à plusieurs types de préjudices. Les attaquants peuvent dérober des informations sous propriété intellectuelle et des documents stratégiques, pouvant nuire à la compétitivité. Le vol de données client peut induire une perte de clientèle, une réputation ternie et un recours juridique. Le vol d'informations médicales privées ou de données financières peut engendrer des problèmes de conformité à la réglementation.

Un programme holistique de protection contre les APT a pour atout secondaire sa contribution à la défense de l'organisation contre d'autres menaces, allant d'attaques externes automatisées à des menaces internes. Nombre de techniques employées pour atténuer l'impact des APT limitent également l'accès aux comptes internes, y compris pour les administrateurs. En limitant l'accès et en séparant les fonctions, même pour les utilisateurs à forts privilèges, l'organisation se protège contre tout administrateur non autorisé ou utilisateur interne malveillant.

Cette approche est unique dans le sens où elle ne requiert aucune connaissance spécifique des vulnérabilités et des nouveaux exploits, et ne repose pas sur la défense d'un périmètre. Grâce à ces techniques, les organisations peuvent appliquer un modèle de sécurité et autoriser ou interdire certaines actions sur la base de règles métier, du niveau de sensibilité des données et de l'anormalité d'un comportement. Ce modèle pouvant être appliqué de façon uniforme sur différentes plates-formes et séparé de la sécurité du système d'exploitation, il peut constituer un moyen efficace pour se protéger contre les APT et détecter les attaques à un stade plus précoce.

---

**Section 4 :**

## Conclusions

Les attaques ciblées sont de plus en plus fréquentes. Les failles de sociétés telles que RSA ont été largement rendues publiques et auront d'importantes conséquences, tant sur leur réputation que sur leur rentabilité.

Le concept de défense approfondie n'est pas neuf. Il s'agit d'un élément fondamental pour tout programme de sécurité. La nouveauté réside dans le rôle central joué par la sécurité des identités internes à forts privilèges dans la prévention des préjudices causés par des attaquants externes. Si le périmètre réseau n'est plus le bastion de la sécurité, l'aspect de l'identité a gagné en importance. Ainsi, « l'identité est devenue le nouveau périmètre ».

Lorsque la notion d'identité est utilisée pour assurer la sécurité contre les menaces internes et externes, telles que les APT, la « prise en compte du contenu » doit être une exigence clé. En utilisant l'intelligence de données pour toute prise de décision d'accès, les organisations d'aujourd'hui peuvent mieux comprendre les risques associés à chaque action de l'utilisateur. Les demandes d'accès à des données sensibles peuvent être analysées et comprises avec un contexte bien plus pointu qu'auparavant. Au lieu d'autoriser ou de bloquer certaines actions selon des règles rigides, les données peuvent être utilisées pour créer une image bien plus claire de l'activité des utilisateurs.

Pour aider votre organisation à prendre l'avantage lorsqu'il s'agit de se défendre contre des attaques ciblées, vous devez adopter un programme de sécurité axé sur la gestion des identités à forts privilèges et la prise en compte du contenu.

**Section 5 :**

## Références


1 http://taosecurity.blogspot.com/2010/01/what-is-apt-and-what-does-it-want.html

2 NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments : http://csrc.nist.gov/publications/drafts/800-30-rev1/SP800-30-Rev1-ipd.pdf

3 « Advanced Persistent Threat », Wikipedia, http://fr.wikipedia.org/wiki/Advanced_Persistent_Threat

4 http://www.rsa.com/node.aspx?id=3872

5 http://fr.wikipedia.org/wiki/Op%C3%A9ration_Aurora

6 http://www.nytimes.com/2010/11/29/world/29cables.html?_r=2&hp


**Section 6 :**

## À propos de l'auteur

Russell Miller travaille depuis plus de huit ans dans le domaine de la sécurité des réseaux, et ce à différentes fonctions, allant du piratage contrôlé ("ethical hacking") au marketing produits. Il est actuellement directeur du marketing produit chez CA Technologies et se consacre principalement à la gestion des identités à forts privilèges et à la protection des données. Russell est titulaire d'une licence en sciences informatiques du Middlebury College et d'une maîtrise en administration des entreprises de la Sloan School of Management du MIT.

ca technologies

**Restez connecté à CA Technologies sur ca.com/fr**

CA Technologies (NASDAQ : CA) crée des logiciels qui alimentent la transformation des entreprises et leur permettent de saisir toutes les opportunités de l'économie des applications. Le logiciel est au cœur de chaque activité et de chaque industrie. De la planification au développement, en passant par la gestion et la sécurité, CA Technologies collabore avec des entreprises partout dans le monde afin de transformer la façon dont nous vivons, interagissons et communiquons, dans les environnements mobiles, de Cloud public et privé, distribués et mainframe. Pour en savoir plus, rendez-vous sur **ca.com/fr**.

Copyright © 2014 CA. Tous droits réservés. Microsoft, SharePoint et Windows sont des marques commerciales ou déposées de Microsoft Corporation aux États-Unis et/ou dans d'autres pays. Linux® est la marque déposée de Linus Torvalds aux États-Unis et dans d'autres pays. Unix est une marque déposée de The Open Group. Tous les noms et marques déposées, dénominations commerciales, ainsi que tous les logos référencés dans le présent document demeurent la propriété de leurs détenteurs respectifs. Ce document est uniquement fourni à titre d'information. CA décline toute responsabilité quant à l'exactitude ou l'exhaustivité des informations qu'il contient. Dans les limites permises par la loi applicable, CA fournit le présent document « tel quel », sans garantie d'aucune sorte, expresse ou tacite, notamment concernant la qualité marchande, l'adéquation à un besoin particulier ou l'absence de contrefaçon. En aucun cas, CA ne pourra être tenu pour responsable en cas de perte ou de dommage, direct ou indirect, résultant de l'utilisation de ce document, notamment la perte de profits, l'interruption de l'activité professionnelle, la perte de clientèle ou la perte de données, et ce même dans l'hypothèse où CA aurait été expressément informé de la survenance possible de tels dommages.

CS200_94805_1014