Application du Principe de Moindre Privilège aux Comptes Utilisateurs sur Windows XP

Publication: Janvier 2006 (Anglais), Avril 2006 (Publication de la traduction française)

Please direct questions and comments about this guide to secwish@microsoft.com.

Commentaires sur la version française: jerome.athias@free.fr

https://www.securinfos.info

To view comments or discussion of this guide, see http://blogs.technet.com/secguide.

Microsoft

Table des Matières

Introduction

Les avancées récentes dans les technologies réseau comme la connexion permanente à Internet ont apportées d'énormes opportunités aux organisations de toute taille. Malheureusement, une connexion entre un ordinateur et n'importe quel réseau, et plus particulièrement Internet, augmente le niveau de risque lié au programmes malicieux et attaquants externes, et alors que les anciens risques sont gérés, de nouveaux sont découverts ou créés.

Sophos, une compagnie de sécurité Internet, a constaté que le nombre de programme malicieux détectés est passé de 45 879 en Novembre 1999 à 114 082 en Novembre 2005, soit une augmentation d'au moins 10% par an durant les six dernières années. En Novembre 2005, Sophos a découvert plus de 1900 nouveaux exemples de programmes malicieux, comme les virus, chevaux de Troie, et spywares. Les autres éditeurs d'antivirus ont également constaté une telle augmentation du nombre de programmes malicieux.

Un facteur significatif qui augmente les risques des programmes malicieux est la tendance à donner aux utilisateurs des droits administratifs sur leurs ordinateurs clients. Lorsqu'un utilisateur ou un administrateur se connecte avec les droits administratifs, chaque programme qu'il exécute, comme les navigateurs, les clients de messagerie, et les logiciels de messagerie instantanée, possèdent également les droits administratifs. Si ces programmes activent un programme malicieux, ce programme malicieux peut s'installer lui-même, manipuler les services comme les programmes antivirus, et même se rendre invisible du système d'exploitation. Les utilisateurs peuvent exécuter des programmes malicieux inconsciemment, par exemple, en visitant un site web compromis ou en cliquant sur un lien dans un message email.

Les programmes malicieux posent de nombreux problèmes aux organisations, de l'interception des informations d'authentification d'un utilisateur avec un enregistreur des touches tapées, à la prise de contrôle totale d'un ordinateur ou d'un réseau en utilisant un rootkit. Les programmes malicieux peuvent rendre un site web inaccessible, détruire ou corrompre des données, et reformater des disques durs. Les effets peuvent inclure des coûts additionnels comme la désinfection des ordinateurs, la restauration de fichiers, la recréation des données perdues. Les attaques des virus peuvent également entraîner des équipes de projet à dépasser des délais, entraînant des ruptures de contrats ou perte de confidentialité des clients.

Les organisations sujettes à la confidentialité peuvent être poursuivies et condamnées.

L'approche Moindre Privilège au Compte Utilisateur

L'approche LUA assure que les utilisateurs suivent le principe de moindre privilège et s'authentifient toujours avec des comptes utilisateurs limités. Cette stratégie vise également à limiter l'utilisation des informations d'authentification administratives aux seuls administrateurs, et ce, uniquement pour accomplir des tâches administratives.

L'approche LUA peut mitiger significativement les risques liés aux programmes malveillants et configuration incorrecte accidentelle. Malgré tout, du fait que l'approche LUA nécessite une planification, des tests et un support des configurations d'accès limités de la part des organismes, cette approche peut engendrer des coûts significatifs. Ces coûts peuvent inclure le redéveloppement de certains programmes, des changements de procédures opérationnelles, et le déploiement d'outils additionnels.

Important **Il est difficile de trouver des outils et supports sur l'utilisation de comptes utilisateurs limités, ainsi ce livre blanc fait référence à des outils et documents tiers. Microsoft ne garantie pas l'efficacité des outils ou des documents pour votre environnement. Vous devez tester chacun de ces instructions ou programmes avant**

de les déployer. Comme avec tous les problèmes de sécurité, il n'y a pas de réponse parfaite, et ce programme ou document ne fait pas exception.

Public Visé

Ce livre blanc est destine à deux catégories:

- Les décideurs qui ont besoin de comprendre les concepts de l'approche LUA et les problèmes organisationnels qu'implique l'approche LUA.
- Les professionnels informatiques qui nécessitent de comprendre les options pour implémenter l'approche LUA dans leur organisation.

Sujets

Ce document traite les problèmes que les organisations peuvent rencontrer lorsqu'elles appliquent l'approche LUA aux ordinateurs qui exécutent Microsoft® Windows® XP. Les aspects suivants sont abordés :

- Risques associés aux privilèges administratifs
- Définition du principe de privilège minimum
- Définition de l'approche LUA
- Bénéfices de l'approche LUA
- Risque, sécurité, usabilité et réduction des coûts
- Implémentation de l'approche LUA
- Développements Futures

Ce document décrit également les problèmes de haut niveau qui affectent l'implémentation de l'approche LUA et fournit des liens utiles vers d'autres ressources en ligne qui expliquent ces concepts plus en détails.

Note Ce document ne traite pas des problèmes d'exécution des services systèmes avec des comptes peu privilégiés. Pour plus d'informations sur ce sujet, se référer à The Services and Service Accounts Security Planning Guide, sur www.microsoft.com/technet/security/topics/serversecurity/serviceaccount/default.mspx

Risques Associés aux Privilèges Administratifs

Beaucoup d'organisations ont l'habitude de donner aux utilisateurs les droits administratifs à leurs ordinateurs. Ceci est particulièrement commun pour les ordinateurs portables, et survient habituellement pour les raisons suivantes :

- Pour exécuter certains programmes correctement. Certains programmes ne peuvent s'exécuter que si un utilisateur dispose des droits administratifs. Typiquement, cela survient si le programme stocke des données utilisateur dans la base de registre ou à des endroits du système de fichiers q'un compte non administrateur ne peut pas accéder.
- Pour permettre à l'utilisateur de réaliser des tâches administratives, comme changer la zone de temps de l'ordinateur.
- Pour permettre aux utilisateurs mobiles d'installer des logiciels ou matériels relatifs à leur travail, comme des imprimantes ou graveurs DVD et les programmes associés.

Il peut y avoir d'autres raisons valides pour octroyer les droits administratifs aux utilisateurs, comme un arrangement.

Considérez la situation dans laquelle un senior effectue régulièrement des visites chez les clients pour effectuer des présentations à l'aide de son ordinateur portable. Du fait qu'il s'agisse d'un senior, il insiste pour avoir les droits administratifs locaux sur son ordinateur. Il est juste en train de faire une présentation décisive à un client important, quand un message offensif apparaît sur l'écran de son portable, qui se verrouille. Quand il redémarre son ordinateur, il constate que le disque dur a été reformaté. En conséquence, il perd le marché au profit d'un concurrent.

Dans ce cas, le message offensif et la destruction de données qui en découle résultent d'un programme malicieux qui a infecté l'ordinateur quand la personne a visité un site web compromis. Quand il a visité ce site, il était authentifié sur l'ordinateur portable comme un membre du groupe local Administrateurs. Les droits et privilèges de ce groupe ont permis au programme malveillant de désactiver le logiciel antivirus, de s'installer, manipuler la base de registre, et placer des fichiers dans le répertoire système de Windows. L'ordinateur était alors compromis, et prêt à exécuter les commandes du programme malicieux.

D'autres scenarii qui exploitent les plus hauts privilèges à partir des comptes administratifs incluent des situations dans lesquelles les utilisateurs cliquent sur des liens dans des mails ou écoutent des CDs de musique qui incluent un logiciel de gestion de droits. Le facteur commun est que les utilisateurs qui possèdent des droits administratifs sont significativement plus en clin à compromettre leurs ordinateurs que ceux qui utilisent des comptes d'utilisateurs limités.

Définition du Principe de Moindre Privilège

Le Critère du Système d'Evaluation de Fiabilité d'un Ordinateur du Département de la Défense, (The Department of Defense Trusted Computer System Evaluation Criteria, (DOD-5200.28-STD)), aussi connu en tant que Livre Orange (Orange Book), est un standard reconnu pour la sécurité informatique. Cette publication définit le privilège minimum comme un principe qui « requiert que chaque sujet dans un système se voit attribué l'ensemble de privilèges les plus restrictifs requis pour la réalisation des tâches autorisées. L'application de ce principe limite les dommages qui peuvent résultés d'un accident, d'une erreur, ou d'une utilisation non autorisée. »

Définition de l'Approche LUA

Ce document définit l'approche LUA comme l'implémentation pratique du principe de privilège minimum sur les ordinateurs sous Windows XP. Particulièrement, les utilisateurs, programmes et services sur Windows XP devraient avoir uniquement le minimum de droits et permissions requis pour réaliser leurs tâches assignées.

Note Il est important de comprendre la différence entre les droits et les permissions. Les droits définissent les tâches qu'un utilisateur peut réaliser sur un ordinateur, alors que les permissions définissent ce qu'un utilisateur peut faire sur un objet de l'ordinateur. Par conséquent, un utilisateur a besoin du *droit* d'éteindre un ordinateur, et d'une *permission* pour accéder à un fichier.

L'approche LUA est une combinaison de recommandations, outils, et bonnes pratiques qui permettent aux organisations d'utiliser les comptes non administratifs pour gérer les ordinateurs qui tournent sous Windows XP. L'approche LUA requière que les organisations réévaluent le rôle des ordinateurs et le niveau d'accès que les utilisateurs devraient avoir sur leur équipement. Elle règle également les considérations stratégiques et quotidiennes de l'utilisation sous des comptes utilisateur limité, et règle les problèmes surgissent. Ces problèmes incluent par exemple des cas comme les utilisateurs distants qui ont besoin de faire des changements de configuration sur leurs ordinateurs.

L'approche LUA devrait également s'appliquer au développement et test d'applications. Les développeurs (et parfois les testeurs) s'authentifie généralement sur leurs ordinateurs avec des comptes qui ont les droits administratifs. Cette configuration peut amener des développeurs à compiler des programmes qui requièrent des privilèges aussi élevés pour s'exécuter. Au lieu de

redéfinir l'application correctement, les développeurs recommandent des « security workarounds », comme placer les comptes utilisateurs dans le groupe local Administrateurs ou accorder aux utilisateurs le contrôle total sur les répertoires Windows.

L'approche LUA contrecarre la tendance simplement en accordant les droits et permissions administratifs à tous les utilisateurs ou programme qui requièrent l'accès à une ressource. Les programmes qui suivent le principe de privilège minimum ne tentent pas d'empêcher les requêtes légitimes aux ressources, mais n'accorde cet accès uniquement en concordance avec une bonne pratique de sécurité.

Pour plus d'informations sur les meilleures pratiques lors de la création d'une application, se reporter à Running with Special Privileges, sur http://msdn.microsoft.com/library/default.asp?url=/library/en-us/secbp/security/running_with_special_privileges.asp.

Comptes Windows XP

Pour comprendre les principes induits par l'approche LUA, vous devez être au fait des différences entre les comptes administratifs et non administratifs dans Windows XP et savoir comment Windows démarre et exécute des programmes. Il est également nécessaire de jeter un oeil sur les groupes dans les réseaux en groupe de travail (workgroup) et avec domaine.

Les ordinateurs sous Windows XP maintiennent une base de sécurité autonome dans le gestionnaire de sécurité locale (Security Accounts Manager : SAM). Le SAM est responsable du stockage des informations sur l'es utilisateurs et groupes locaux, et inclus plusieurs groupes par défaut, comme :

- **Administrateurs**. Possèdent un accès complet et non restreint à l'ordinateur.
- **Utilisateurs avec Pouvoir**. Possèdent des droits administratifs plus limités, comme partager des fichiers, installer des imprimantes locales et changer l'heure du système. Ils possèdent également des permissions étendus pour accéder aux fichiers dans les répertoires systèmes de Windows.
- **Utilisateurs**. Possèdent des droits utilisateur limités empêchant des changements accidentaux et intentionnels du système. Les comptes utilisateurs qui sont membres de ce groupe sont *seulement* référencés comme *comptes utilisateurs limités*.
- **Invités**. Possèdent moins de droits que les utilisateurs.

Les comptes utilisateurs obtiennent leurs droits en étant membre d'un ou plusieurs de ces groupes. Par exemple, le compte Administrateur inclus par défaut possèdent les droits administratifs car il est membre du groupe Administrateurs. Cette appartenance à ce groupe donne au compte Administrateur des droits élevés, comme le droit de forcer l'arrêt d'un ordinateur à distance depuis un autre ordinateur.

L'ordinateur base sur un groupe de travail est entièrement autonome et ne valide que les groupes et utilisateurs dans son propre SAM. Quand un ordinateur d'un groupe de travail joint un domaine, les appartenances de groupes locales changent. En plus des groupes existants, le groupe Utilisateurs du Domaine devient un membre du groupe local Utilisateurs et le groupe Administrateurs du Domaine devient un membre de Administrateurs. Ce changement permet n'importe quel membre du groupe Administrateurs du Domaine à s'authentifier sur l'ordinateur avec les droits administratifs, et n'importe quel membre du groupe Utilisateurs du Domaine à s'authentifier sur l'ordinateur avec les droits utilisateur limité.

Comptes Administratifs

Un compte administratif est un compte qui est membre d'au moins un des groupes administratifs. Sur un ordinateur joint à un domaine, les groupes administratifs incluent :

- Le groupe local des Administrateurs
- Le groupe local des Utilisateurs avec Pouvoir
- Le groupe Administrateurs du Domaine
- Le groupe Opérateurs de Configuration du Réseau
- N'importe quel groupe qui est membre d'un groupe administratif local

N'importe qui, s'authentifiant comme membre d'un ou plusieurs de ces groupes peut réaliser des modifications systèmes.

Note Le groupe Utilisateurs avec Pouvoir est une sous-catégorie de Administrateurs plutôt qu'une sur-catégorie du groupe Utilisateurs. Placer des utilisateurs dans le groupe Utilisateurs avec Pouvoir ne correspond pas aux principes de LUA.

Utilisateurs Limités

Un utilisateur limité est un compte qui est membre du groupe local Utilisateurs et n'est *pas* un membre d'un groupe administratif. Sur un ordinateur joint à un domaine, n'importe quel membre du groupe Utilisateurs du Domaine est aussi un membre du groupe local Utilisateurs.

Les comptes utilisateurs limités réduisent significativement la surface d'attaque pour les programmes malicieux du fait que ces comptes possèdent le minimum de possibilité d'effectuer des modifications du système qui affectent la sécurité opérationnelle. En particulier, les comptes utilisateurs limités ne peuvent pas ouvrir de port au niveau du pare-feu, ni arrêter ou lancer des services, ni modifier les fichiers dans les répertoires système de Windows.

Beaucoup d'organisations diront qu'elles implémentent déjà l'approche LUA car leurs utilisateurs s'authentifient comme membres du groupe Utilisateurs du Domaine. Néanmoins, si ces utilisateurs sont également des membres du groupe local Administrateurs, tous les programmes qu'ils exécutent auront les privilèges administratifs et peuvent potentiellement entraîner des modifications non souhaitées.

Comprendre le Processus d'Authentification

Une autre domaine à comprendre est le processus d'authentification sur Windows XP. Quand un utilisateur s'authentifie sur un ordinateur, le système d'exploitation authentifie les informations d'authentification de l'utilisateur et lance une instance du bureau Windows, la plupart du temps Windows Explorer. Ce bureau s'exécute dans le contexte de sécurité de l'utilisateur avec les droits d'accès et permissions de l'utilisateur authentifié. Quand l'utilisateur exécute un programme, comme Microsoft Internet Explorer, ce programme s'exécute également dans le contexte de sécurité de l'utilisateur.

S'authentifier comme Administrateur

Si un utilisateur s'authentifie comme un membre du groupe local Administrateurs, le bureau et tous les programmes que l'utilisateur exécute vont s'exécuter avec les droits d'accès et permissions complets d'un administrateur. Les utilisateurs qui possèdent les droits administratifs peuvent réaliser les actions suivantes, qui sont légitimement requises pour administrer un ordinateur :

- Installer, lancer et arrêter des services et des pilotes de périphériques.
- Créer, modifier et supprimer le registre.
- Installer, exécuter et désinstaller des programmes.
- Remplacer des fichiers du système d'exploitation.
- Terminer des processus.

- Contrôler la configuration du pare-feu.
- Gérer les entrées du gestionnaire d'événements.
- Installer des contrôles Microsoft ActiveX®.
- Accéder au SAM.

Pour la majorité des utilisateurs d'ordinateur, ces droits sont inutiles et augmentent significativement les risques. De par le fait qu'un utilisateur avec les droits administratifs peut réaliser ces modifications du système, un programme qu'un utilisateur avec les droits administratifs exécute, intentionnellement ou par accident, le peut aussi. Ainsi, si un utilisateur s'authentifie avec les droits administratifs, il est beaucoup plus facile pour un programme malicieux de s'installer sur l'ordinateur.

S'authentifier comme simple Utilisateur

Les utilisateurs qui ne sont pas membres du groupe Administrateurs peuvent seulement accéder à un nombre réduit de ressources, puis peuvent ne pouvoir effectuer des modifications que sur des zones particulières. Pour comparer les droits utilisateurs avec les droits administratifs, les utilisateurs peuvent réaliser les tâches suivantes :

- Voir l'état des services et pilotes de périphériques.
- Créer, modifier, et supprimer des éléments du registre dans **HKEY_CURRENT_USER**, et lire des éléments dans **HKEY_LOCAL_MACHINE**.
- Exécuter des programmes.
- Lire la plupart des fichiers du système d'exploitation.
- Voir les processus en cours d'exécution.
- Voir la configuration du pare-feu.
- Voir les entrées (logs) d'événements système et application uniquement.

Les utilisateurs limités peuvent toujours effectuer des tâches qui leurs sont requises pour faire leur travail, comme se joindre à un réseau sans-fil, installer des pilotes Plug and Play signés. L'approche LUA ne cherche pas à limiter ces possibilités, mais à réduire les risques en limitant les comptes qui possèdent les droits administratifs.

Vous devriez désormais comprendre le rôle des groupes dans Windows XP et les différences entre l'authentification avec les droits utilisateurs administratifs et limités.

Bénéfices de l'approche LUA

L'approche LUA apporte de nombreux bénéfices aux organisations de toute taille. En plus de la réduction des risques face aux attaques par des programmes malicieux, ces bénéfices incluent :

- Amélioration de la sécurité
- Amélioration de la gestionabilité
- Amélioration de la productivité
- Réduction des coûts
- Réduction des problèmes légaux et de piraterie

Cette section analyse ces bénéfices et comment ils peuvent affecter votre organisation.

Amélioration de la sécurité

L'approche LUA est l'une des nombreuses mesures de sécurité qui peut aider à protéger votre organisation et ses ordinateurs contre l'exploitation par des attaquants. Les attaquants cherchent à compromettre votre réseau pour différentes raisons, qui peuvent comprendre :

- Obtenir l'accès à plusieurs ordinateurs pour les utiliser dans des attaques par déni de service distribuées.
- Envoyer du spam.
- Compromettre des informations de propriété industrielle.
- Voler les identités des utilisateurs.
- Distribuer des programmes malicieux à d'autres ordinateurs.

Ces attaques ont plus de chances d'aboutir quand l'utilisateur s'authentifie avec un compte qui possèdent les droits administratifs. Par exemple, un programme qui s'exécute avec les droits administratifs peut :

- Installer des rootkits en mode kernel.
- Installer des programmes de niveau système enregistrant les touches frappées. (keyloggers)
- Intercepter les mots de passe.
- Installer un spyware et adware.
- Accéder à des données appartenant à d'autres utilisateurs..
- Exécuter du code quand quelqu'un s'authentifie.
- Remplacer des fichiers système par des chevaux de Troie.
- Réinitialiser les mots de passe.
- Couvrir ses traces dans les logs d'événements.
- Empêcher l'ordinateur de redémarrer.

Si les utilisateurs s'authentifient avec de comptes d'utilisateur limité, les programmes qui s'exécutent dans ces contextes utilisateur ne peuvent uniquement effectuer des modifications mineures sur le système d'exploitation. L restriction réduit significativement la possibilité pour les programmes malicieux de s'installer et s'exécuter, ce qui améliore la sécurité sans empêcher les utilisateurs de faire leur travail.

Amélioration de la Maniabilité

La standardisation est un composant important d'un réseau maniable, particulièrement avec plusieurs ordinateurs clients. Si une organisation possède 500 ordinateurs clients, et que chaque ordinateur possède une configuration logicielle différente et des paramètres différents, la gestion proactive devient extrêmement complexe. Cette complexité survient inévitablement quand les utilisateurs installent des logiciels et font des modifications du système.

Windows XP fournit un énorme potentiel pour paramétrer le système d'exploitation. Si les utilisateurs peuvent s'authentifier avec les droits administratifs, ils succombent souvent à la tentation de modifier des paramètres. Par exemple, un utilisateur peut désactiver le pare-feu pour une connexion réseau sans-fil, puis se connecter à internet par le biaise d'une connexion insécurisée d'un point d'accès public. Cette action peut conduire à une compromission rapide de l'ordinateur, de part le fait que toutes les connections réseau (même à des réseaux fiables) doivent être protégées par un pare-feu.

Les modifications initiées par un utilisateur tendent à générer plus d'appels au support, et à chaque fois qu'un ordinateur modifié requière de l'attention, le personnel du support fait face a

une configuration différente. Ce manque de standardisation rend la tâche de maintenance et réparation plus difficile, plus consommatrice de temps et plus chère.

L'approche LUA crée également des limites de gestion clairement définies entre les utilisateurs et les administrateurs. Cette limite permet aux utilisateurs de se concentrer à faire leur travail, pendant que les administrateurs du réseau gère l'infrastructure. Si les utilisateurs possèdent les droits administratifs, il devient impossible d'imposer cette limite, et la standardisation ne peut pas être garantie.

Un réseau dans lequel tout le monde est administrateur est effectivement ingérable, du fait que les utilisateurs peuvent dérégler les paramètres du système. Si les utilisateurs ne peuvent pas installer de matériel ou programmes non autorisés, leurs ordinateurs devraient rester raisonnablement cohérents au standard organisationnel. L'approche LUA améliore la maniabilité en limitant les modifications non désirées des environnements informatiques.

Amélioration de la Productivité

Les ordinateurs ont apporté une énorme amélioration de la productivité pour les organisations de tout genre et taille. Néanmoins, les ordinateurs requièrent une gestion proactive pour maintenir cet avantage de productivité. Dans les organisations pour lesquelles les utilisateurs dépendent de leur ordinateur pour travailler, l'équipe informatique doit minimiser la probabilité de disfonctionnement, particulièrement ceux dus à des causes évitables comme des configurations d'ordinateur incorrectes et infections par un programme malicieux.

L'approche LUA peut maintenir la productivité à travers la maintenance des configurations des ordinateurs clients. Quand les utilisateurs ne peuvent pas changer la configuration de leurs ordinateurs, ces ordinateurs sont plus stables, ce qui conduit à une réduction du temps de panne et maintient la productivité.

Une perte de productivité peut également survenir quand un programme malicieux prend le contrôle d'un ordinateur. L'ordinateur peut nécessiter une désinfection ou même un reformatage, et l'utilisateur peut perdre ces documents ou données du fait de l'infection. Les administrateurs peuvent avoir à restaurer des sauvegardes des fichiers, qui devront ensuite être mis à jour. Ces activités additionnelles peuvent distraire les employés de leurs tâches principales ou nécessiter de réeffectuer un travail déjà accompli.

Coûts Réduits

Bien que la maintenance de plusieurs ordinateurs clients ne puisse être gratuite, les facteurs suivants peuvent significativement augmenter les coûts :

- Une combinaison unique et non testée de matériel et logiciel
- Des modifications inconnues sur le système d'exploitation
- Des paramètres système personnalisés
- Un logiciel non standard avec un format de fichier inconnu
- Des licences pour un logiciel installé par un utilisateur
- Un logiciel installé sans licence
- Un programme malicieux
- Un logiciel ou pilote en version beta
- Utilisation de la bande passante internet par un programme malicieux

L'approche LUA aide à prévenir l'installation de programmes non autorisés, non enregistrés, ou malicieux. Cela empêche également les utilisateurs de faire des modifications inconnues sur

leurs ordinateurs. Cela limite les coûts de maintenance et temps d'arrêt que les utilisateurs avec les droits administratifs peuvent causer.

Réduction des Problèmes de piratage et Responsabilité Légale

Organizations are increasingly aware of their regulatory compliance obligations to prevent illegal use of company equipment by employees. These obligations require companies to take action when employees either knowingly or unknowingly:

Les organisations s'intéressent de plus en plus à leurs obligations de conformité pour empêcher l'utilisation illégale des équipements de la société par les employés. Ces obligations nécessitent que les sociétés prennent des mesures quand les employés, de manière volontaires ou involontaires :

- Permette le vol de données client
- Hébergent des sites web qui contiennent du contenu piraté, illicite ou offensant
- Hébergent des serveurs relais pour du Spam
- Prennent part dans des attaques distribuées par déni de service (denial-of-service attacks).

Les organisations qui implémentent l'approche LUA sont significativement moins de chance d'être tenus pour responsables par ces types d'abus, car leurs ordinateurs clients sont plus difficiles à compromettre.

En plus de cela, les utilisateurs ont moins de chance d'être capables d'installer des programmes non autorisés pour héberger du contenu illégal, ce qui diminue significativement les chances de les voir commettre de tels actes pour entrainer un telle responsabilité. Cette sauvegarde entraîne les utilisateurs limités à ne posséder que la lecture seule sur le répertoire Program Files, les répertoires système Windows, et à la section **HKEY_LOCAL_MACHINE** du registre. Les programmes nécessitent en général l'accès en écriture pour s'installer.

Risque, Sécurité, Maniabilité, et Coût

Comme beaucoup d'approches de gestion réseau, l'adoption des méthodes LUA implique de mesurer les différences entre le risque, la sécurité, la maniabilité, et le coût. Une fois bien implémentée, l'approche LUA peut :

- Réduire le risque.
- Améliorer la sécurité.
- Impacter la maniabilité.
- Réduire les coûts d'administration.

Réduction du Risque

N'importe quelle connexion à un ordinateur encoure un risque, et les connexions à Internet encore plus que celles à des ressources intranet. La seule manière d'écarter complètement ce risque est de ne pas connecter un ordinateur à un réseau. La plupart des organisations s'accordent sur le fait que les bénéfices de la connectivité réseau dépasse les risques, mais les stratégies qui minimisent ces risques sont à prendre en considération.

L'approche LUA peut conduire à une réduction significative des risques actuels et futurs qui résultent de l'exécution de programmes avec les droits administratifs. Les organisations qui n'appliquent pas l'approche LUA augmentent non seulement les risques liés à l'utilisation de

l'ordinateur, mais aussi la vulnérabilité face à de nouveaux exploits, particulièrement les exploits « zero-day » où les attaquants découvrent une vulnérabilité dans une application avant le concepteur. Les organisations qui mettent en place l'approche LUA sont probablement mieux disposées à mettre en place d'autres stratégies de gestion, comme les mises à jour automatiques, qui réduisent encore plus le risque.

Amélioration de la Sécurité

L'approche LUA apporte une sécurité grandement améliorée. La différence est de réduire la liberté pour l'utilisateur de faire des modifications de configuration, mais non nécessairement réduire la facilité d'utilisation.

Il est important de comprendre que l'approche LUA ne fournit pas une stratégie de sécurité complète, mais doit s'intégrer avec d'autres défenses de sécurité comme une stratégie de stratégie en profondeur. Ces défenses multiples incluent l'éducation des utilisateurs, des pare-feu, des mises à jour de sécurité régulières, et des scanners à jour pour détecter les programmes malicieux. L'approche LUA fournit une sécurité additionnelle qui réduit la possibilité pour un programme malveillant de se propager au sein de l'organisation.

Impact sur la Maniabilité

Il est couramment dit que pour la gestion réseau, la facilité d'utilisation et la sécurité sont inversement proportionnelles l'une de l'autre, et qu'augmenter la sécurité réduit la facilité d'utilisation.

Note La considération importante est que la facilité d'utilisation doit être de la simplicité, et ne doit pas être la possibilité pour l'utilisateur d'effectuer les modifications qu'il souhaite sur son ordinateur.

L'approche LUA empêchent les utilisateurs d'administrer leurs ordinateurs, pas de les utiliser. Leur retirer les droits administratifs rend les utilisateurs plus productifs, du fait qu'ils ont moins de distractions et réduit les opportunités de configurer leurs ordinateurs de manière incorrecte.

Malgré tout, si l'utilisateur peut voir une option de configuration, mais pas la changer, cela peut être une source de frustration et peut générer des appels au service technique. La Politique de Groupe (Group Policy) vous permet de masquer des éléments de l'interface Windows à l'utilisateur. Si les utilisateurs ne voient que les options qu'ils peuvent changer, les restrictions de configuration deviennent significativement moins frustrantes. L'implémentation de l'approche LUA en conjonction avec la Politique de Groupe vous permet de créer une interface simplifiée qui n'affiche que les options que l'utilisateur peut modifier.

Réduction des Coûts d'Administration

Des études menées par des organismes indépendants ont démontrées les gains sur long terme que la gestion des systèmes réseau peuvent procurer. L'approche LUA se rapproche d'une stratégie de gestion de systèmes car les utilisateurs limités ne peuvent pas modifier les paramètres de gestion imposés. Néanmoins, pour réaliser les économies de la gestion de systèmes, les organisations doivent être préparées à faire l'investissement que l'approche LUA nécessite, et comprendre les coûts de l'implémentation ou non de l'approche LUA.

Implémenter l'approche LUA implique des coûts pour :

- Planifier et piloter le projet.
- Tester des programmes dans un environnement LUA.
- Rechercher des solutions pour les comptes utilisateur limité.
- Réécrire des applications si nécessaire.
- Tester les nouveaux programmes avant déploiement.

- Prévoir l'augmentation initiale des appels au support.
- Régler les problèmes politiques de ce changement.

Il est important de confronter ces coûts avec ceux engendrés par la non implémentation de l'approche LUA. Ne pas implémenter LUA peut créer des coûts de par :

- Des configurations d'ordinateur incorrectes engendrées par des modifications de l'utilisateur.
- Des programmes non autorisés, non testés, non enregistrés, ou malicieux.
- Des ennuis légaux potentiels.
- Des pertes de marché dues à des compromissions de sécurité.

L'analyse des coûts entre l'implémentation et la non implémentation démontre que la plupart des coûts d'implémentation sont chiffrables, alors que les coûts de non implémentation sont inconnus. Il est possible d'évaluer le coût de réécriture d'une application de ligne de marché, mais impossible d'estimer le coût d'un procès.

La rapide évolution des menaces pour les ordinateurs en réseau et la nécessité de simplifier et standardiser les configurations informatiques va grandement encourager les organisations et particuliers à exécuter leurs réseaux et ordinateurs sous des comptes utilisateur limité. Les arguments pour l'approche LUA s'introduisent maintenant significativement dans l'inertie organisationnelle et la mauvaise pratique établie. Il est maintenant nécessaire de revoir la manière dont les organisations peuvent implémenter l'approche LUA.

Implémenter l'approche LUA

L'implémentation de l'approche LUA implique l'application des règles suivantes aux ordinateurs sous Windows XP:

- Les non administrateurs doivent toujours s'authentifier comme utilisateurs limités.
- Les administrateurs doivent utiliser uniquement des comptes administratifs pour réaliser des tâches administratives.

Bien que cette approche apporte les bénéfices déjà présentés par ce documents et impose un environnement fiable, de nombreuses considérations doivent être réglées, particulièrement quand une organisation a préalablement autorisé des utilisateurs à s'authentifier en tant qu'administrateurs.

Considérations de l'Implémentation

Implémenter l'approche LUA génère également des problèmes techniques, administratifs et politiques au sein de l'organisation. Ceux-ci incluent :

- Le contrôle sur l"ordinateur
- L'installation de matériel
- L'installation de programmes
- L'exécution de programmes
- La mise à jour du système d'exploitation
- La configuration du système d'exploitation
- Les coûts

Contrôle sur l’Ordinateur

Probablement le plus difficile des problèmes politiques auquel faire face, est le contrôle sur les ordinateurs clients. Beaucoup de seniors et preneur de décisions prévoient un contrôle total sur leurs ordinateurs, et sont ignorants des risques inhérents à cette configuration. Les personnes qui tiennent une place de direction sont souvent intolérants face aux situations qui les frustrent ou aux messages qui leurs disent ce qu’ils ne peuvent pas faire. Une réponse typique à n’importe quel message à propos d’une restriction de droits est d’insister pour que l’administrateur réseau leur donne un contrôle administratif total.

Pour gérer cette situation, il est essentiel de posséder un commanditaire exécutif convenablement éduqué techniquement et hiérarchiquement important pour le projet. Pour beaucoup d’entreprises, ce commanditaire exécutif doit être au moins le chef de service de l’information (Chief Information Officer : CIO) ou équivalent, et disposé à éduquer sur la menace grandissante représentée par un programme malicieux et comment de tels programmes peuvent s’installer depuis un site web malicieux ou compromis. Si l ‘éducation ne produit pas un argument suffisamment puissant, mettez en avant les problèmes légaux qui peuvent résulter de l’installation non intentionnelle d’un programme malveillant sur leurs ordinateurs, et expliquez comment les outils de ce document peuvent résoudre tous leurs soucis.

L’éducation des utilisateurs est un autre domaine à régler. La plupart des utilisateurs vont se sentir menacés par n’importe quelle tentative de leur enlever le contrôle de ce qu’il voit comme « leur » ordinateur, et peuvent perturber l’implémentation de l’approche LUA. Il est courant de recevoir un grand nombre de complaintes mêlées d’exagération des problèmes que les utilisateurs rencontrent du fait qu’ils ne disposent plus des droits administratifs. Tant que l »organisation a réalisé un plan de test, ces complaintes peuvent être réglées facilement.

Installation de Matériel

Les utilisateurs avec un ordinateur de bureau ne devraient pas disposer des droits administratifs sur leur lieu de travail. Néanmoins, les utilisateurs nomades peuvent légitimement avoir besoin d’installer du matériel comme des imprimantes ou graveurs DVD pour faire leur travail quand ils ne sont pas connectés au réseau de l’entreprise.

Le problème de l’installation de matériel pour les utilisateurs nomades est un de ceux pour lesquels l’organisation nécessite de considérer les options possibles, incluant des options possibles qui ne correspondent pas à l’approche LUA. Les outils que décrit ce document, dans la prochaine section, peuvent également assister la gestion de cette situation.

Installation de Programmes

Beaucoup de programmes nécessitent les droits administratifs pour s’installer. Ce comportement aide à inhiber l’installation de programmes non autorisés, mais peut aussi empêcher l’installation de programmes et mises à jour autorisées. L’installation d’un programme peut être particulièrement problématique quand un utilisateur n’a pas un ordinateur joint à un domaine ou se connecte seulement occasionnellement au réseau de l’organisation. La résolution de ce problème peut requérir des modifications des procédures opérationnelles et l’utilisation d’outils comme la publication d’application dans Active Directory®, le Elevated Rights Deployment Tool dans Microsoft Systems Management Server (SMS) 2003 avec Service Pack 1, ou le bureau à distance (Remote Desktop).

Certains sites internet ne fonctionnent correctement qu’avec des logiciels additionnels et des contrôles ActiveX qui se téléchargent sur l’ordinateur client. Les outils de gestion comme le Kit d’Administration d’Internet Explorer et les Politiques de Groupe peuvent permettre ce comportement avec des sites où le besoin financier est plus grand que le risque perceptible face au téléchargement de logiciels depuis cet emplacement.

Exécuter des Programmes

Certains programmes nécessitent les privilèges administratifs pour s'exécuter. Typiquement, cette restriction découle d'erreurs de programmation ou d'une mauvaise implémentation des bonnes pratiques de programmation et sécurité. Par exemple, un programme peut installer une clé de produit obligatoire dans le registre où un compte utilisateur limité ne peut pas lire la valeur de la clé.

Note Les programmes qui suivent les recommandations Microsoft ne devraient pas rencontrer de problèmes de restrictions de sécurité.

Dans bien des cas, il est possible de palier au problème en accordant au groupe Utilisateurs l'accès à l'endroit restreint qui pose problème. Le Microsoft Windows Application Compatibility Toolkit (ACT) que ce document décrit dans la section suivante peut également palier à beaucoup de ces problèmes d'incompatibilité. Les administrateurs réseau ne devraient pas simplement accepter que du fait qu'un programme ne fonctionne qu'avec les permissions administratives, tout le monde doit être administrateur.

Mettre à Jour le Système d'Exploitation

L'installation manuelle des mises à jour de système d'exploitation depuis le site Microsoft Update requière que le bureau du système d'exploitation soit exécuté avec les droits administratifs, donc, pour utiliser Microsoft Update, l'utilisateur doit s'authentifier avec les informations d'authentifications administratives. Néanmoins, le service de Mises à jour Automatiques tourne sous les privilèges système et ne rencontre pas cette restriction. Si vous configurez les Mises à jour automatiques pour vérifier et installer les mises à jour du système d'exploitation et des programmes automatiquement, il ne devrait que rarement être nécessaire de mettre à jour manuellement. Pour plus d'informations, voir How to schedule automatic updates in Windows Server 2003, in Windows XP, and in Windows 2000, sur http://support.microsoft.com/default.aspx?scid=kb;en-us;327838.

SMS 2003 avec le Service Pack 1 inclut des fonctionnalités pour identifier et installer les mises à jour du système d'exploitation et d'applications sans que l'utilisateur ne dispose des droits administratifs. Windows Software Update Services (WSUS) fournit une gestion simplifiée des mises à jour de sécurité pour les organisations qui n'ont pas SMS d'installé.

Configurer le Système d'Exploitation

La politique informatique de l'organisation se doit de définir quelles actions de configuration les utilisateurs limités peuvent réaliser sur leurs ordinateurs. Les modifications des politiques de sécurité (security policies) et paramètres registre, localement ou par la Politique de Groupe, peuvent permettre aux utilisateurs limités de faire des modifications approuvées sur leur ordinateur, tout comme les utilisateurs mobiles nécessitent de changer l 'heure ou la zone horaire de leur ordinateur. La section suivante de ce document liste différents outils qui résolvent le problème de la configuration du système d'exploitation avec un compte utilisateur limité.

Coûts

Finalement, l'approche LUA peut être chère à planifier, implémenter et gérer. If you have third party or custom line-of-business or mission-critical programs, these costs can be significant.

Un exemple peut être un programme critique qui n'est pas compatible avec l'approche LUA et requière les droits administratifs pour s'exécuter. En fonction de l'age du programme et des disponibilités des développeurs, l'organisation pourrait être amené à :

- Tester le programme dans un environnement LUA.
- Identifier un processus de mitigation si le programme ne s'exécute pas comme:

  - Personnaliser les permissions du registre ou modifier les permissions sur plusieurs ordinateurs.
  - Changer les droits d'accès.
  - Déployer des outils pour palier aux problèmes de configuration.
- Réécrire le programme depuis le départ.

Néanmoins, si l'organisation a déjà planifier de mettre à jour le programme personnalisé en une technologie récente, le coût de conformité à l'approche LUA peut être insignifiant.

Outils

De nombreux outils sont disponibles via Microsoft ou d'autres éditeurs pour assister la gestion d'un environnement qui utilise l'approche LUA. Cette section décrit quelques utilitaires qui aide à gérer les environnements dans lesquels les utilisateurs s'authentifie avec des droits utilisateur limités. Ces outils incluent :

- Secondary Logon service
- MakeMeAdmin
- PrivBar
- PolicyMaker
- Application Compatibility Toolkit
- RegMon et FileMon
- Systems Management Server

Note MakeMeAdmin, Privbar, PolicyMaker, RegMon, et FileMon ne sont pas supportés par Microsoft, et Microsoft n'assure aucune garantie sur la fiabilité de ces programmes. Utiliser ces programmes est entièrement à vos propres risques.

Secondary Logon Service

The Secondary Logon service (ou la commande *runas*) permet aux utilisateurs d'exécuter des programmes avec des informations d'authentification alternatives. Le Secondary Logon service créée un autre jeton (token) de sécurité avec les nouvelles informations d'authentification et d'appartenance de groupe, dont va se servir le programme pour accéder aux ressources.

Bienque le Secondary Logon service est un outil utile, le deuxième compte utilise des informations d'authentification séparées du premier compte, ce qui crée les restrictions suivantes:

- L'utilisateur doit connaitre le mot de passé du second compte, et doit soumettre ces informations d'authentification.
- Certains programmes ne peuvent pas exécuter une seconde instance avec des informations d'authentification différentes de l'instance courante.
- Le deuxième compte ne doit pas avoir les mêmes mappings d'imprimantes ou périphériques que le premier compte.
- Le deuxième compte doit être un compte local, et donc ne pas avoir de droits d'accès au réseau ou aux ressources du domaine, ni ne pouvoir exécuter de scripts logon du domaine, ou appliquer de Politique de Groupe.
- Certaines modifications (comme l'installation de programmes) ne s'appliquent qu'au profil du second compte, pas au premier. Cet effet peut intervenir quand un programme s'installe pour « Cet utilisateur seulement » (This user only) plutôt que pour « Tous les utilisateurs » (All users).

La commande *runas* ne fonctionne pas quand elle est dirigée pour utiliser des chemins UNC (Universal Naming Conventio), comme les connexions aux imprimantes ou réseau. Il y a des contournements qui résolvent ce problème, comme utiliser la commande *runas* pour lancer Internet Explorer, puis ouvrir des objets basés sur des répertoires dans Internet Explorer. Néanmoins, cette approche complique la simplicité de l'approche « clic droit, **Run As** ».

Les autres utilisations de la commande *runas* incluent la création d'un raccourci vers un script dans le menu **Envoyer vers** (Send To) de l'utilisateur, qui lance le programme sélectionné avec les droits administratifs. Les raccourcis peuvent également avoir l'option avancée **Exécuter en tant que** (Run with different credentials). Pour plus d'informations, voir How to enable and use the "Run As" command when running programs in Windows sur http://support.microsoft.com/default.aspx?scid=kb;en-us;294676&sd=tech.

Lien ajouté à la traduction française:

http://download.microsoft.com/download/8/b/1/8b136f49-3e5d-4913-9454-6c5abfb5df4e/Principe-du-moindre-privilege-en-action.ppt

MakeMeAdmin

MakeMeAdmin évite les restrictions de drive mapping, droits d'accès, et installation de programme du Secondary Logon service à travers l'utilisation de deux processus d'authentification successifs. Pour éviter ces restrictions, le script:

1. Obtient le détail de vos informations d'authentification courantes
2. Invoque le Secondary Logon service ainsi vous pouvez vous authentifier avec les informations d'authentification du compte local Administrateur.
3. Utilise la nouvelle session de l'Administrateur locale pour ajouter votre compte courant dans le groupe Administrateurs local.
4. Invoque une fois de plus le Secondary Logon service et vous invite à vous authentifier avec votre compte utilisateur courant, mais comme un membre du groupe local Administrateurs.
5. Créée une nouvelle invite de commandes dans laquelle votre compte courant est un membre du groupe local Administrateur. Cette invite de commande possède une couleur de fond et un titre différents pour la distinguer d'une invite de commande standard.
6. Retire votre compte courant du groupe local Administrateurs.

L'invite de commande que créée le script s'exécute sous les informations d'authentification de votre courant mais avec les droits administratifs, et n'importe quel programme que vous exécutez depuis cette invite de commandes possède également les droits administratifs. Vos drive mappings et droits d'accès réseau sont les mêmes que votre compte courant et si vous utiliser cette invite de commande pour installer un programme, celui ci s'installera dans votre profil courant, pas dans le profil Administrateur.

Pour plus d'informations sur MakeMeAdmin, voir MakeMeAdmin -- temporary admin for your Limited User account sur le blog de Aaron Margosis, sur http://blogs.msdn.com/aaron_margosis/archive/2004/07/24/193721.aspx.

PrivBar

PrivBar affiche une barre d'outils colorée dans Internet Explorer et Windows Explorer qui montre le niveau de privilège courant de l'utilisateur. Par exemple, si un utilisateur s'authentifie avec les droits administratifs, la barre d'outils PrivBar apparaît en jaune, avec un indicateur rouge. Cet indicateur rappelle aux utilisateurs qu'ils utilisent les privilèges administratifs pour naviguer sur un site web, ce qui augmente le risque pour leur ordinateur. Pour plus d'informations sur PrivBar, voir PrivBar -- An IE/Explorer toolbar to show current privilege level sur le blog de Aaron Margosis, sur http://blogs.msdn.com/aaron_margosis/archive/2004/07/24/195350.aspx

PolicyMaker

PolicyMaker de Desktop Standard consiste en une suite d'utilitaires qui étendent la possibilité de Politique de Groupe à permettre l'approche LUA avec des réseaux distribués. La suite PolicyMaker inclut également des outils pour vérifier et fixer les problèmes de compatibilité de programmes. Les outils les plus significatifs pour implémenter l'approche LUA comprennent PolicyMaker Standard Edition, PolicyMaker Application Security, et PolicyMaker Software Update.

PolicyMaker Application Security est d'un intérêt particulier pour l'approche LUA. Il permet aux administrateurs réseau d'attacher des niveaux de permissions à des programmes individuels. L'administrateur réseau sélectionne le programme, puis retire les groupes de sécurité du jeton de processus quand le programme est exécuté. Cette restriction se propage ensuite à travers la Politique de Groupe. Pour plus d'informations sur PolicyMaker, voir PolicyMaker Overview sur le site de Desktop Standard Web, sur www.desktopstandard.com/PolicyMaker.aspx.

Application Compatibility Toolkit

Microsoft Windows Application Compatibility Toolkit (ACT) est une collection d'outils et documents qui assistent les professionnels informatiques et développeurs dans la réalisation des plus hauts niveaux de compatibilité avec les systèmes d'exploitation Windows. Les outils incluent:

- **Application Analyzer**. Cet outil simplifie l'inventaire de l'application et les tests de compatibilité.
- **Compatibility Administrator**. Cette base de données liste les correctives de compatibilité necessaries pour supporter des programmes dépassés sur Windows.
- **Internet Explorer Compatibility Evaluator**. Cet outil fournit des logs détaillés sur Internet Explorer qui enregistre les problèmes de compatibilité avec ce navigateur.

Compatibility Administrator inclut des outils qui permettent à un développeur de vérifier les problèmes de permission utilisateur pendant la phase de développement d'applications personnalisées. ACT peut générer un correctif de compatibilité que l'administrateur peut déployer sur les ordinateurs des utilisateurs. Ce correctif de compatibilité permet alors au programme de s'exécuter en mode LUA en redirigeant les appels de l'application vers des endroits où l'utilisateur limité possède un accès en lecture et écriture. Pour plus d'informations sur ACT, voir Windows Application Compatibility sur www.microsoft.com/technet/prodtechnol/windows/appcompatibility/default.mspx.

RegMon et FileMon

RegMon et FileMon sont deux utilitaires proposés par le site web respecté Sysinternals. Regmon affiche en temps réel l'activité d'accès à la base de registre, listant tous les appels au registre qu'une application effectue, et enregistre les résultats. Cette outil vous permet d'identifier quand une application ne peut pas accéder à une clé du registre. De la même manière, FileMon affiche en temps réel l'activité du système de fichier, listant tous les appels systèmes qu'une application réalise et enregistre les résultats.

RegMon et FileMon permettent aux administrateurs de tester une application avec l'environnement LUA et d'identifier les échecs d'appels au registre ou système de fichiers que l'application peut rencontrer. L'administrateur peut ensuite mitiger cet échec, par exemple, en changeant les permission à la clé de registre ou du système de fichiers. Les Polices de Groupe peuvent propager ces changements permissions à plusieurs ordinateurs. Pour plus d'informations sur ces utilitaires, se rendre sur le site Sysinternals à www.sysinternals.com.

Systems Management Server

Microsoft Systems Management Server (SMS) 2003 est un système de gestion de bureau complet qui fournit des services de gestion pour les organisations moyennes et grandes avec des réseaux centralisés ou distribués. Ces services de gestion incluent l'installation de logiciels et de mises à jour de sécurité.

SMS fournit un support pour l'approche LUA à travers la possibilité d'installer des logiciels et des mises à jour de sécurité sans nécessité que les utilisateurs s'authentifient avec des droits administratifs. Pour plus d'informations sur SMS, voir Systems Management Server 2003 SP1 Product Overview sur www.microsoft.com/smserver/evaluation/overview/default.mspx.

Limiter les Informations d'Authentification Administratives

Si une organisation n'est pas à même d'implémenter l'approche LUA entièrement, il est possible de mitiger le risque de voir exécuter des programmes avec des droits administratifs en s'assurant que les programmes qui accèdent à des ressources réseau s'exécutent toujours avec des droits utilisateur limité. Bien que cette approche ne satisfait pas avec le principe de moindre privilège, elle offrir certains bénéfices, et est meilleure que de simplement permettre à tout le monde d'exécuter des programmes avec des droits administratifs.

Pour fournir une sécurité réelle quand les utilisateurs s'authentifient avec les droits administratifs, vous devrez:

- Déployer des outils pour minimiser les risques d'exécuter des programmes en tant qu'administrateur
- Vous assurer que les programmes liés à internet, comme les clients de messagerie, les navigateurs et messageries instantanées s'exécutent toujours avec des droits utilisateur limité. Autoriser ces programmes avec des droits administratifs est la méthode la plus courante pour introduire un programme malveillant dans une organisation.
- Surveiller les ordinateurs pour une utilisation administrative non approuvée. Pour plus d'informations sur la surveillance sécurité, voir The Security Monitoring and Attack Detection Planning Guide, sur www.microsoft.com/technet/security/topics/auditingandmonitoring/securitymonitoring/default.

Les outils suivants aident à minimiser le risque de compromission d'un ordinateur quand les utilisateurs s'authentifient avec les droits administratifs. En plus de cela, certains des outils de la section « S'authentifier comme un Utilisateur Limité » s'appliquent également à cette situation.

- Secondary Logon service
- Software Restriction Policies
- DropMyRights

Note DropMyRights n'est pas supporté par Microsoft, et Microsoft ne garantit aucunement la fiabilité de ce programme. Utilisez ce programme à votre propre risque.

Secondary Logon Service

Le Secondary Logon service fournit une option pour exécuter un programme sous un compte moins privilégié. Par exemple, sur Windows XP avec SP2, les icônes du bureau de l'utilisateur pour Internet Explorer peuvent être remplacées avec des versions qui invoquent la boite de dialogue Exécuter en tant que, qui affiche ensuite l'option **Protéger mon ordinateur de l'activité de programmes non autorisés.** Cette option désactive les identificateurs de sécurité (security identifiers : SIDs) dans le jeton d'accès de l'utilisateur d'une manière équivalente à l'outil DropMyRights décrit plus loin dans cette section.

Restriction des Politiques Logicielles

Les politiques de restriction logicielle font partie de la Politique de Groupe (Group Policy) et fournissent la possibilité de réguler les programmes inconnus et non sûrs. Les politiques de restriction logicielles peuvent appliquer un des trois paramètres possibles aux programmes. Ces paramètres sont :

- Unrestricted
- Disallowed
- Basic user

Note Seulement Unrestricted et Disallowed sont visibles par défaut. Pour voir le paramètre Basic user, vous devez éditer une clé du registre. Pour plus d'informations, voir Browsing the Web and Reading E-mail Safely as an Administrator, Part 2, sur http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dncode/html/secure01182005.asp.

En résumé, les programmes non restreints peuvent s'exécuter sans obstacle, les programmes non permis ne peuvent pas, et les programmes qui possèdent le paramètre Basic user peuvent seulement s'exécuter avec les droits utilisateur limité. Cette approche vous permet, par exemple, de configurer une politique de restriction logicielle qui exécute toujours Internet Explorer en tant qu'utilisateur limité.

Les politiques de restriction logicielle peuvent également prévenir l'exécution d'un programme malicieux depuis certains endroits, comme le répertoire de fichiers temporaires d'Internet Explorer. Une règle de restriction de chemin logicielle peut empêcher n'importe quel programme qui tente de s'exécuter depuis le répertoire temporaire d'Internet. La Politique de Groupe peut appliquer cette règle à tous les ordinateurs dans le domaine.

Pour plus d'informations sur les politiques de restriction logicielle, voir Using Software Restriction Policies to Protect Against Unauthorized Software, sur www.microsoft.com/technet/prodtechnol/winxppro/maintain/rstrplcy.mspx.

DropMyRights

DropMyRights désactive les SIDs et retire les privilèges du jeton d'accès utilisateur, puis utilise ce jeton restreint pour lancer un programme spécifié. DropMyRights permet à un utilisateur de s'authentifié avec les droits administratifs puis d'exécuter un programme avec un de ces 3 niveaux de privilèges :

- Normal
- Contraint (Constrained)
- Non fiable (Untrusted)

Note le niveau de privilèges *normal* correspond à un compte utilisateur limité. Le niveau *constrained* est plus restreint du fait de l'ajout de SIDs restreints au jeton d'accès. Le niveau *untrusted* possède seulement les droits minimums, et la plupart des applications ne fonctionneront pas à ce niveau.

Par exemple, un utilisateur avec les privilèges administratifs peut avoir besoin de visiter un site web. L'utilisateur peut exécuter Internet Explorer depuis un raccourci qui invoque DropMyRights, et ce raccourci va spécifier que le programme doit s'éxécuter en mode contraint. Cette instance d'Internet Explorer aura alors les droits minimum sur l'ordinateur client, ce qui réduit fortement les risques qu'un programme malveillant puisse s'exécuter ou s'installer.

Pour plus d'informations sur DropMyRights, voir Browsing the Web and Reading E-mail Safely as an Administrator, sur http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dncode/html/secure11152004.asp.

Pour plus d'informations sur les effets d'exécuter Internet Explorer en tant qu'utilisateur restreint, voir Running restricted -- What does the "protect my computer" option mean? sur http://blogs.msdn.com/aaron_margosis/archive/2004/09/10/227727.aspx.

Développements Futurs

Windows Vista inclue des fonctionnalités qui vont améliorer la protection des comptes utilisateurs. Windows Vista va permettre aux utilisateurs de travailler réellement avec des comptes utilisateur limité, et les programmes certifies Windows Vista n'auront pas de problème à s'exécuter sous des comptes utilisateur limité. Quand d'anciens programmes essayeront d'écrire dans des emplacements protégés comme la section **HKEY_LOCAL_MACHINE**, Windows Vista redirigera ces écritures dans la section **HKEY_CURRENT_USER** à la place. Néanmoins, comme les éditeurs mettent à jour leurs programmes et les certifient pour Windows Vista, cette opération sous l'approche LUA devrait devenir monnaie courante.

Windows Vista améliore également la facilité d'utilisation. Si un utilisateur tente de réaliser une modification qui nécessite les droits administratifs, Vista demande automatiquement à l'utilisateur d'entrer les informations d'authentification administratives.

Une protection accrue pour les comptes utilisateurs est juste une des améliorations majeures pour la sécurité dans Windows Vista. Les risques d'exploitation des comptes de niveau administrateur par des programmes malveillants devraient diminués dans les organisations migrant vers Windows Vista. Pour plus d'informations sur la protection de compte utilisateur dans Windows Vista, voir le site de Windows Vista sur www.microsoft.com/windowsvista/it-professionals.mspx.

Résumé

L'augmentation des menaces pour les ordinateurs en réseau requière que les organisations de toutes les tailles implémentent une stratégie de défense en profondeur. Implémenter l'approche LUA sur des ordinateurs fonctionnant sous Windows XP fournit un composant important de cette stratégie.

L'approche LUA contre la tendance de beaucoup d'organisations à accorder les droits administratifs aux utilisateurs d'ordinateurs clients via l'appartenance au groupe local Administrateurs. Ce document souligne les dangers inhérents au fait de donner les droits administratifs à tous les utilisateurs, du fait que cela confère les privilèges administratifs à n'importe quel programme que l'utilisateur exécute. Il est particulièrement important que des programmes reliés à internet comme les navigateurs, les clients de messagerie et de messagerie instantanée ne soient pas exécutés habituellement avec les droits administratifs, car cette configuration rend l'ordinateur client significativement plus vulnérable à une attaque.

To return briefly to the example at the beginning of this paper, if the organization had implemented l'approche LUA, the executive would have browsed the compromised Web site as a limited user rather than as an administrator. Le programme malicieux n'aurait pas du être capable d'infecter son ordinateur portable et le représentant aurait du être capable de conclure sa vente.

Finalement, l'approche LUA n'est pas une solution en elle-même, mais doit s'intégrer avec d'autres défenses de sécurité. Ces défenses incluent la prise de conscience utilisateur, des pare-feux, des mises à jour de sécurité régulières, et des scanners à jour pour détecter des programmes malicieux.

Ressources

Pour plus d'informations sur l'utilisation de l'approche LUA sur Windows XP, consultez les ressources suivantes:

- Blog de Aaron Margosis sur http://blogs.msdn.com/aaron_margosis
- Blog de Michael Howard sur http://blogs.msdn.com/michael_howard

- Le site nonadmin sur http://nonadmin.editme.com
- Le Administrator Accounts Security Planning Guide sur www.microsoft.com/technet/security/topics/serversecurity/administratoraccounts/default.mspx
- Le newsgroup Windows XP Security and Admin. sur TechNet sur www.microsoft.com/technet/community/newsgroups/dgbrowser/en-us/default.mspx?dg=microsoft.public.windowsxp.security_admin.
- TechNet Webcast: Limited User Access: The Good, the Bad and the Ugly (Level 300) sur http://msevents.microsoft.com/CUI/WebCastEventDetails.aspx?EventID=1032278618&EventCategory=5&culture=en-US&CountryCode=US
- TechNet Webcast: Tips and Tricks to Running Windows with Least Privilege (Level 300) sur http://msevents.microsoft.com/CUI/WebCastEventDetails.aspx?EventID=1032274954&EventCategory=5&culture=en-US&CountryCode=US
- Le Microsoft Security Developer Center sur http://msdn.microsoft.com/security/default.aspx
- Le livre blanc Developer Best Practices and Guidelines for Applications in a Least Privileged Environment sur http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnlong/html/AccProtVista.asp
- L'article Developing Software in Visual Studio .NET with Non-Administrative Privileges sur http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dv_vstechart/html/tchDevelopingSoftwareInVisualStudioNETWithNon-AdministrativePrivileges.asp
- Writing Secure Code, Second Edition par Michael Howard sur www.microsoft.com/MSPress/books/5957.asp
- L'article How to Troubleshoot Program Compatibility Issues in Windows XP sur www.microsoft.com/technet/prodtechnol/winxppro/support/troubleshoot.mspx
- Department of Defense Trusted Computer System Evaluation Criteria (Orange Book) sur www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html
- Cette traduction sur https://www.securinfos.info

Remerciements

The Microsoft Solutions for Security and Compliance group (MSSC) would like to acknowledge and thank the team that produced *Applying the Principle of Least Privilege to User Accounts on Windows XP*. The following people were either directly responsible or made a substantial contribution to the writing, development, and testing of this solution.

Author

Anthony Steven, *Content Master Ltd*

Writer

Mike Danseglio

Testers

Gaurav Singh Bora, *Infosys Technologies*

Mehul Mediwala, *Infosys Technologies*

Editors

Jennifer Kerns, *Wadeware*

John Cobb, *Volt Information Sciences*

Program Manager

Tom Cloward

Release Manager

Flicka Crandell

Contributors

Tony Bailey

Darren Canavor

Karl Grunwald

Kelly Hengesteg

Karina Larson, *Volt Information Sciences*

Chrissy Lewis, *Siemens Business Services, Inc.*

David Mowers

Jeff Newfeld

Bomani Siwatu

Stacy Tsurusaki, *Volt Information Sciences*

David Visintainer, *Volt Information Sciences*

Reviewers

Bob Blank, *Target Corporation*

Jeremy Brayton, an independent reviewer

Derick Campbell

Chase Carpenter

Ramulo A. Ceccon, *Dataprom*

Matt Clapham

Chris Corio

Greg Cottingham

John Czernuszka

Michael Dragone, *Titleserv, Inc*

Dana Epp, an independent reviewer

Stephen Friedl, *Microsoft Security MVP*

Guido Grillenmeier, *Hewlett-Packard*

Michael Harradon, *Netivity Solutions*

Robert Hurlbut, *Hurlbut Consulting, Inc*

Mark Kradel

Jamie Laflen

Alex Lee, *Sprint Nextel Corporation*

Kevin Lundy, *CAE, Inc*

Tim C. MalcomVetter, *Truman Medical Centers*

Aaron Margosis

Brian Marranzini

David McClure, *Siemens Medical Solutions*

Don McGowan

Michael Miller, *Media General, Inc*

Charles J. Palmer, an independent reviewer

Keith Pawson, an independent reviewer

Brian A. Reiter, *WolfeReiter, LLC*

Michael Rickard, *Bristol University*

John Robbins, *Wintellect*

Alex Rublowsky

Mike Smith-Lonergan

Mike Sorsen, *Edward Jones*

Didier Stevens, *Contraste Europe*

Eric Wood

Martin Zugec, an independent reviewer