

Les 7 règles d'or pour déployer Windows 7

Les premiers rapports sont tombés et il est évident que Microsoft Windows 7 démarre fort, en partie grâce au programme bêta libéral de Microsoft et à la forte demande qui existait au sein des utilisateurs de Vista et XP pour un nouveau système d'exploitation. La part de marché de Windows 7 a déjà atteint les 6 %, chiffre que le spécialiste en études de marché Net Applications attribue à une demande croissante pour une sécurité accrue, des délais d'initialisation plus courts, une plus grande stabilité et une meilleure aisance d'utilisation.

Jonathan Tait, Responsable du Marketing Produit, Sophos
et Jason De Lorme, ISV Architect Evangelist, Microsoft

Les 7 règles d'or pour déployer Windows 7

Introduction

Les premiers rapports sont tombés et il est évident que Microsoft Windows 7 démarre fort, en partie grâce au programme bêta libéral de Microsoft et à la forte demande qui existait au sein des utilisateurs de Vista et XP pour un nouveau système d'exploitation. La part de marché de Windows 7 a déjà atteint les 6 %, chiffre que le spécialiste en études de marché Net Applications attribue à une demande croissante pour une sécurité accrue, des délais d'initialisation plus courts, une plus grande stabilité et une plus grande facilité d'utilisation.

Les 7 recommandations pour optimiser la sécurité dans Windows 7

Si vous prévoyez de déployer Microsoft Windows 7 dans un avenir proche, il serait judicieux de revoir auparavant la protection des données et des systèmes d'extrémité de tous les ordinateurs du réseau opérant sous Windows, quelle que soit la version installée. Il y a plusieurs recommandations que toute entreprise devrait suivre, quelle que soit sa taille, dans le but de protéger ses machines Windows des conséquences potentiellement désastreuses d'une attaque de virus, spyware ou autre forme de malware.

1. Neutraliser les menaces

Une étape élémentaire mais néanmoins primordiale est d'utiliser un antivirus pour empêcher, détecter et supprimer tous les différents types de malware qui présentent un danger considérable pour vos systèmes et données.

L'un des moyens les plus répandus de détecter un virus est de rechercher des formules récurrentes connues ou des signatures dans le code exécutable. Il reste néanmoins possible qu'un utilisateur soit infecté par un nouveau malware pour lequel il n'existe pas encore de signature en raison de l'augmentation du nombre de menaces et la complexité des malwares inconnus. Pour contrer ces menaces "du jour zéro", il est important de s'équiper d'un antivirus proactif qui identifie les nouveaux virus en étudiant leur comportement et qui les empêche de s'exécuter.

Pour s'assurer qu'un antivirus soit à la hauteur de ses attentes, il est impératif de le garder à jour. Un nouveau virus peut se propager rapidement, c'est pourquoi il est important d'avoir en place une infrastructure automatique, capable de mettre à jour tous les ordinateurs du réseau fréquemment, rapidement et en toute transparence de manière à rester aux devants des menaces les plus récentes.

Une autre façon très simple de se protéger des menaces est de rester informé. Inscrivez-vous sur la liste de distribution de votre éditeur d'antivirus et consultez les blogs sur la sécurité pour vous tenir au courant des dernières menaces de virus et des informations techniques, et tout savoir sur le support disponible et les nouveautés en cours de développement.

Recommandations

La fonction DEP (Data Execute Prevention) empêche le code de s'exécuter dans les zones de mémoire destinées au stockage des données. Nous vous recommandons de vérifier la configuration de votre BIOS pour activer la prise en charge du DEP (activer NX) et ce, pour toutes les applications.

La fonction ASLR (Address Space Layout Randomization) sélectionne aléatoirement les emplacements dans la mémoire de votre ordinateur utilisés par Windows pour charger les bibliothèques système essentielles. Cette fonction, associée au DEP, limite le fonctionnement des malwares en les empêchant d'exploiter les vulnérabilités dans votre navigateur, vos plugins et vos applications.

En déployant Sophos Endpoint Security and Data Protection sur le système Windows 7, vous bénéficiez d'une sécurité accrue. Sophos fournit un système runtime de prévention des intrusions sur l'hôte (HIPS) qui surveille le comportement de vos applications lorsqu'elles sont actives. Ce contrôle renforce la protection contre les malwares du jour zéro en recherchant les comportements malveillants avant même qu'une signature ait été créée.

La console d'administration centralisée de Sophos, l'Enterprise Console, vous permet de surveiller, mettre à jour et gérer votre sécurité depuis un point unique afin de garantir que votre logiciel antivirus est bien opérationnel, à jour et conforme aux politiques dans toute votre entreprise. Ainsi, vous êtes sûr que vos ordinateurs Windows 7 sont sécurisés et vous pouvez facilement programmer des contrôles de détection des malwares lorsque les postes ne sont pas utilisés.

2. Garantir une navigation Internet sûre

L'internet est devenu un outil indispensable pour un grand nombre d'entreprises. Résultat : de nombreux sites légitimes deviennent des cibles pour les auteurs de malwares et les pirates qui infectent les postes des visiteurs afin de leur dérober des informations professionnelles confidentielles, de propager du code malveillant ou même de créer des réseaux zombies pour la distribution de spam ou de malware.

Des milliers de systèmes sont infectés chaque jour par des utilisateurs qui consultent des sites de confiance ayant fait l'objet d'attaques SQL qui exploitent les vulnérabilités et injectent du code malveillant.

Ouvrir l'accès à Internet tout en maintenant la productivité des salariés et garantissant une protection efficace contre les menaces potentielles est un défi difficile à relever. Cependant, vous pouvez commencer par prendre de simples mesures.

Recommandations

Windows 7 s'accompagne par défaut de la version 8 d'Internet Explorer, et est protégé à la fois par les fonctions DEP et ASLR. De plus, il introduit une nouvelle fonction de sécurité, appelée SmartScreen, qui protège en cas de navigation sur des sites malveillants. SmartScreen lance un avertissement lorsque l'utilisateur se dirige vers des sites contenant du script "cross-site", du phishing et autres destinations malveillantes connues. Ces fonctions, associées au mode de protection de IE 8, assurent une navigation plus sûre.

D'autre part, Sophos renforce cette sécurité avec la fonction BHO (Browser Helper Object) qui se connecte à Internet Explorer pour analyser le contenu dynamique des sites Web et détecter le code malveillant et les failles. Si du code dangereux est détecté, une alerte apparaît à l'utilisateur et elle est enregistrée dans l'Enterprise Console qui centralise l'édition des rapports et la journalisation.

De plus, vous pouvez renforcer la protection de vos ordinateurs avec une appliance de sécurité qui neutralise les malwares et bloque les proxys anonymes et autres applications indésirables à la passerelle. En déployant une sécurité Web par couches, vos ordinateurs sont protégés aussi bien dans l'entreprise qu'à l'extérieur.

3. Maintenir les correctifs à jour

Les pirates peu scrupuleux se consacrent plus que jamais à exploiter les failles existant dans les plugins tiers ou dans toute application qui télécharge du contenu d'Internet. Ils continuent de cibler le système d'exploitation mais recherchent de plus en plus les applications que votre navigateur utilise pour visionner les médias, les documents et autres types de fichiers.

Il est donc important de consulter régulièrement les sites Web des éditeurs d'applications tierces pour vérifier s'ils ont sorti de nouvelles mises à jour. De nombreux éditeurs de logiciels publient également des recommandations de sécurité. Microsoft, par exemple, propose une liste de distribution dédiée aux problèmes et failles de sécurité découverts dans ses logiciels, et fournit des correctifs pour les rectifier. Consultez vos fournisseurs et inscrivez-vous à leur liste de notification pour être sûr d'être tenu au courant des nouveaux problèmes qu'ils découvrent.

Lorsqu'une nouvelle faille est découverte dans une application ou un système d'exploitation et qu'il existe un correctif pour y pallier, les entreprises devraient disposer d'une infrastructure permettant de tester que le correctif fonctionne avant de le déployer sur l'ensemble de leur réseau d'utilisateurs.

Recommandations

En plus de votre logiciel actuel, Windows Update contribue à maintenir vos postes sécurisés en collectant les dernières mises à jour de fonctionnalités et de sécurité de Microsoft via Internet. Dans Windows 7, on le retrouve dans l'Action Center, qui simplifie encore plus le processus de mise à jour.

Pour garantir que Windows Update est activé lorsque les postes sont connectés à votre réseau, vous pouvez utiliser les fonctions de contrôle de la conformité comprises dans Sophos Endpoint Security and Data Protection. Elles évaluent les postes administrés et non administrés et peuvent également vérifier qu'un autre logiciel de sécurité est activé et à jour.

4. Renforcer le DLP (Prévention des pertes de données)

Le but des auteurs de malwares était jusqu'à récemment de s'attirer le plus d'attention possible pour gagner de la notoriété. Une nouvelle tendance se confirme toutefois ces derniers temps. La diffusion de malwares est devenue un crime à part entière dont le but est de se procurer frauduleusement des informations confidentielles. Il est donc sage de prévoir des mesures préventives pour empêcher une fuite regrettable de vos données.

La protection de données se compose de quatre aspects différents :

- » **Le contrôle des applications** permet d'administrer les applications que vous permettez à vos employés d'utiliser. Ceci garantit que vos politiques de sécurité sont respectées à tout moment et que les données sensibles de l'entreprise ne font pas l'objet de fuites au travers d'applications telles que le partage de fichiers en peer-to-peer ou les messageries instantanées.
- » **Le contrôle des périphériques** permet de définir les périphériques autorisés et non autorisés à l'échelle de l'entreprise. Les employés bénéficient de la souplesse dont ils ont besoin sans occasionner de risques pour l'entreprise.
- » **Le contrôle des données** garantit que les utilisateurs ne transfèrent pas accidentellement des données sensibles sur leurs périphériques et leurs applications. La mise en place d'une stratégie de prévention de la fuite de données peut être une opération à la fois coûteuse et complexe, il est donc préférable de chercher une solution qui l'intègre dans sa protection de systèmes d'extrémité.
- » **Le chiffrement** assure la protection des données se trouvant sur les ordinateurs portables et les périphériques USB, car il arrive que les gens perdent du matériel. Le chiffrement de données peut ne pas être aussi simple que l'on pourrait le penser, c'est pourquoi il faut considérer différents facteurs: assurez-vous que la première installation soit réussie, que vous pouvez administrer et modifier les politiques de chiffrement à travers l'ensemble du réseau de l'entreprise, et surtout que la solution que vous utilisez ne gêne en rien le travail quotidien des utilisateurs.

Recommandations

Windows 7 conserve les technologies de protection des données présentes dans Windows Vista telles que l'Encrypting File System (EFS) et la technologie intégrée Active Directory Rights Management Services. Ces technologies offrent une excellente plate-forme pour la protection des données stockées.

Pour les données échangées, Sophos intègre le DLP directement à son logiciel client pour systèmes d'extrémité. Grâce aux fonctions d'administration centralisée de Sophos, toutes les politiques de sécurité peuvent être administrées à l'aide d'une console unique. En un seul contrôle, Sophos Endpoint and Data Protection peut appliquer les règles de DLP en même temps que la recherche de malware et autre contenu suspect.

Windows 7 permet un contrôle des ports USB plus poussé via le déploiement des GPO (Group Policy Objects) qui peuvent vous aider à protéger vos données sensibles. Windows 7 améliore également la technologie BitLocker en introduisant BitLocker To Go, qui permet de déployer le chiffrement sur les lecteurs de disques amovibles FAT32 tels que les clés USB et les disques durs externes.

Sophos Device Control suit le principe de Windows 7 en effectuant des contrôles plus précis, qui vérifient chaque périphérique individuellement, tout en administrant vos politiques utilisant les groupes déjà définis pour les autres fonctions de sécurité.

Windows 7 renforce les contrôles d'applications disponibles dans Windows XP et Vista avec l'introduction d'AppLocker. AppLocker permet aux administrateurs d'adopter une approche de type liste blanche/liste noire pour la gestion des applications, qui s'en trouve allégée car elle ne dépend plus du hachage ou des signatures des applications. Cette procédure permet de simplifier la mise à jour et le déploiement du logiciel en éliminant le besoin d'approuver chaque révision, même mineure.

L'approche de Sophos permet également d'effectuer les mises à jour des applications sans besoin de GPO. Les politiques de Sophos sont administrées via l'Enterprise Console et les SophosLabs s'occupent de définir les applications.

Une fois la politique établie, les SophosLabs mettent à jour en permanence la liste de définitions du logiciel et peuvent même détecter les applications qui sont déjà installées ou qui ne requièrent pas d'installation. Ce type de contrôle des applications ne détecte pas seulement les applications en cours d'installation, mais aussi lors du run-time. Les politiques de Sophos peuvent être appliquées sur les installations Windows XP, Vista et 7, facilitant la transition vers de nouveaux environnements d'exploitation.

Microsoft BitLocker est une fonction de chiffrement intégral du disque comprise dans les éditions Ultimate et Enterprise de Windows Vista Windows 7. Avec la sortie de Windows 7, BitLocker a rajouté une nouvelle fonction de chiffrement des périphériques amovibles. Sophos offre un cadre d'administration qui permet à l'entreprise de gérer de manière centralisée ses postes de travail Windows XP ainsi que les lecteurs chiffrés via BitLocker sur Windows Vista et Windows 7.

5. Administrer les droits utilisateurs

Windows 7 offre plus de possibilités que jamais de garantir un environnement informatique sûr. Avec l'introduction de la fonction UAC (User Account Control), Microsoft donne plus de contrôle aux administrateurs réseau, leur permettant de mieux faire accepter les comptes standards auprès des utilisateurs. Lorsque le contrôle UAC est activé, il empêche les utilisateurs d'apporter des modifications au niveau du système sans l'approbation d'un administrateur. Cela permet de mieux sécuriser les ordinateurs de bureaux face aux attaques de logiciels malveillants qui tirent profit des droits d'administration des utilisateurs, et simplifie également le processus pour les administrateurs souhaitant autoriser les comportements qu'ils savent être sûrs.

En plus de limiter les droits d'administration des utilisateurs, Sophos recommande d'apporter quelques modifications supplémentaires lors du déploiement de Windows 7 pour profiter pleinement de la sécurité renforcée proposée par ce nouveau système d'exploitation.

Par exemple, Microsoft a présenté une fonctionnalité pour mieux administrer la rotation de mots de passe. En combinant deux paramètres, la demande de changement de mot de passe tous les X jours (90 est un bon chiffre par défaut) et la limitation du nombre de mots de passe réutilisables (5 est recommandé), vous pouvez maintenant définir un GPO qui empêche de changer un mot de passe jusqu'à ce qu'il soit expiré. Sophos recommande de tirer le meilleur parti de cette fonctionnalité car elle empêche les utilisateurs de modifier continuellement leur mot de passe pour détourner les politiques et revenir à leurs mots de passe d'origine.

6. Prévenir les failles de sécurité

Avec la mobilité accrue des employés, il est de plus en plus difficile d'assurer que tous les postes de travail, et notamment les ordinateurs portables itinérants, bénéficient de la protection requise pour maintenir votre entreprise sécurisée, les éléments de base étant d'avoir un antivirus à jour et un pare-feu activé.

Sophos recommande de déployer des politiques de sécurité complètes pour vérifier que tout ordinateur accédant au réseau — même ceux n'appartenant à l'entreprise — sont en parfaite conformité. De telles politiques garantissent que seuls les postes répondant à vos exigences de conformité sont autorisés à accéder à votre réseau. S'ils ne répondent pas aux exigences, ils sont bloqués.

Recommandations

Windows 7 : la fonction NAP (Network Access Protection, Protection de l'Accès Réseau), introduite dans Windows Vista, demeure un élément clé de Windows 7. Le NAP a été conçu pour aider les administrateurs à maintenir la bonne santé du parc informatique ce qui, à son tour, contribue à maintenir l'intégrité globale du réseau, mais sa fonction n'est pas de protéger le réseau des utilisateurs malveillants.

Sophos intègre le Network Access Control (NAC) dans sa protection pour systèmes d'extrémité afin de vous aider à identifier les failles potentielles sur les postes administrés et non administrés, vous permettant ainsi de choisir de bloquer un poste non conforme, ou bien d'améliorer la sécurité pour répondre au standard requis avant d'autoriser l'accès.

Le contrôle des applications de Sophos peut également aider les entreprises en garantissant que seules les versions approuvées puissent fonctionner. Vous pouvez spécifier les versions pour lesquelles vous souhaitez autoriser l'exécution, par exemple Internet Explorer 8 et Firefox 3 et non les versions plus anciennes. Cela aide ainsi à protéger votre environnement contre les programmes expirés ou moins sécurisés.

7. Eduquer les utilisateurs

Une bonne stratégie de sécurité doit inclure des règles interdisant :

- » Le téléchargement de fichiers exécutables ou de documents provenant directement du Web ou d'un courriel.
- » L'ouverture de fichiers exécutables, de documents ou de tableaux non sollicités.
- » L'utilisation de jeux ou d'économiseurs d'écran qui n'étaient pas inclus dans le système d'exploitation.

N'oubliez pas que l'efficacité d'une politique de sécurité repose en grande partie sur la performance du logiciel de protection que vous utilisez. Empêchez le personnel de se livrer à des pratiques risquées.

Recommandations

Si ce n'est pas déjà fait, rédigez un guide de la sécurité informatique, que vous distribuerez à l'ensemble du personnel. Assurez-vous que les employés prennent connaissance du document, le comprennent et sachent à qui s'adresser s'ils ont des questions ou si leur ordinateur a fait l'objet d'une attaque ou d'une infection.

Lorsque c'est possible, il est recommandé de bloquer l'accès aux malwares pouvant être véhiculés via email ou téléchargé à partir du Web. On peut citer par exemple les fichiers .exe et .com, .msi, .vbs et .bat. Les technologies telles que les Sophos Email Appliances et les Sophos Web Appliances peuvent également déterminer le type de fichier véritable (True File Type) pour empêcher les utilisateurs de renommer simplement des fichiers dangereux pour les distribuer.

Conclusion

Pour les déploiements en entreprises, Sophos puise dans les fonctions de sécurité du nouveau système d'exploitation de Microsoft, Windows 7, et renforce la gestion globale de la sécurité pour vous permettre de tirer le meilleur profit de votre investissement dans cette nouvelle version.

Combiner les solutions de Microsoft et de Sophos vous aidera à respecter les exigences de conformité interne et externe, à améliorer la sécurité et à bénéficier de l'expertise nécessaire dans les environnements exigeants actuels.

Sophos est un ISV Microsoft certifié Gold, avec des compétences en Sécurité, Mobilité, Information Worker, ISV/Software et Infrastructure Réseau. Sophos s'engage à respecter les normes Microsoft et a commencé la commercialisation de ses produits certifiés Windows 7 le jour du lancement de Windows 7 par Microsoft.

Sophos assure également la compatibilité pour les anciennes plates-formes de Microsoft jusqu'à Windows 98. Cette combinaison vous permet d'assurer une sécurité complète et homogène pour l'ensemble de vos postes Windows.

Boston, Etats-Unis | Oxford, Royaume-Uni

© Copyright 2010. Sophos Plc.

*Toutes les marques déposées et tous les copyrights sont compris et reconnus par Sophos.
Aucune partie de cette publication ne peut être reproduite, stockée dans un système de recherche documentaire ou transmise, sous quelque forme ou par quelque moyen que ce soit sans le consentement préalable écrit de l'éditeur.*

SOPHOS
WWW.SOPHOS.COM