

Protection de votre réseau d'entreprise:
Que savez-vous exactement de vos postes
fixes et mobiles?



Sommaire

Sommaire	1
Résumé	3
Introduction : Les postes de travail non sécurisés sont une source de vulnérabilités majeures	3
Prévention d'intrusions par une analyse des postes	4
La course à la création d'une norme de facto pour la gestion de l'accès au réseau... 4	
Fonctionnalités novatrices de LANDesk® Trusted Access™	6
Protection préventive	8
Gestion proactive grâce à LANDesk® Management Gateway	8
Extension du périmètre de préemption.....	9
Conclusion.....	9
Références.....	9

Le présent document contient des informations confidentielles qui sont la propriété de LANDesk Software (LANDesk) et de ses sociétés affiliées. Ces informations sont fournies pour le(s) produit(s) LANDesk concerné(s). Aucune partie de ce document ne peut être diffusée ou copiée sans l'autorisation écrite préalable de LANDesk. Ce document n'implique la concession d'aucune licence, expresse ou implicite, par forclusion ou autre, concernant les droits de propriété intellectuelle. Sauf mention contraire dans les termes et conditions de vente LANDesk de ces produits, LANDesk décline toute responsabilité, notamment concernant tout brevet, droit de copyright ou autre droit de propriété intellectuelle. Les produits LANDesk ne sont pas destinés à des applications médicales, de secours ou de maintien en vie. LANDesk ne garantit pas que le présent document est exempt d'erreurs. LANDesk se réserve le droit de l'actualiser, de le corriger ou de le modifier, notamment au niveau des spécifications et des descriptions produits, à tout moment et sans préavis.

Copyright © 2006 LANDesk Software, Ltd. Tous droits réservés.

LANDesk® est une marque déposée de LANDesk Software, Ltd. Les autres marques et noms sont la propriété de leurs détenteurs respectifs.
LSI-0435 0106 JBB/KL

Résumé

Les directeurs informatiques sont garants de la sécurisation et de la conformité des biens informatiques de leur entreprise. Outre le fait de devoir se préoccuper de leurs traditionnelles tâches d'administration informatique, ils font désormais face à un éventail des nouveaux défis parmi lesquels le maintien de la sécurité des points d'extrémité, la gestion des machines infectées, l'application de la conformité, la prévention de la prolifération des codes malicieux.

Ce livre blanc examine la manière dont les fonctionnalités LANDesk® Trusted Access™ de mise en quarantaine des postes infectés ou non conformes aident les entreprises à mieux protéger et sécuriser les points d'extrémité du réseau. L'objectif étant de réduire les attaques malicieuses et les temps d'arrêt associés ainsi que la perte de productivité et de revenus.

Introduction: Les postes non sécurisés sont une source de vulnérabilités majeures

Alors que les traditionnels modèles de sécurité informatique sont dédiés à la protection du périmètre réseau, il devient aujourd'hui plus difficile de définir et de défendre ce même périmètre. Dans la plupart des cas l'origine des incidents recensés en entreprise provient d'un non respect des règles de sécurité, intentionnel ou non. Qui plus est, les utilisateurs autorisés à accéder aux ressources informatiques posent davantage de dangers que ceux contraints d'ouvrir une brèche dans le firewall périmétrique pour pénétrer sur le réseau.

Pourquoi ? Parce que les points d'extrémité informatiques tels que les ordinateurs portables, les postes de travail, les PDA et autres équipements mobiles sont souvent vulnérables et susceptibles d'être infectés par un virus. Ils peuvent leur manquer des patches critiques, ou être dépourvus d'un logiciel anti-virus. Les fichiers de signature peuvent également être périmés ou un firewall personnel peut être mal configuré.

Le cabinet Yankee Group Research, Inc., rapporte que l'informatique mobile augmente de manière constante et que le nombre d'employés bénéficiant d'un accès distant est passé de 25% en 2003 à 34% en 2004. Les menaces de sécurité diffusées en internes telles que les logiciels espions, les vers, les chevaux de Troie, les points d'entrée secrets (backdoors), les enregistreurs de touches et tout autre code malicieux sont en augmentation. Ainsi que les nouvelles tactiques. Si vous avez des intentions malveillantes, pourquoi tenter de pénétrer des firewalls ou des passerelles applicatives lorsque vous pouvez abuser des utilisateurs de confiance ? ¹

Les scénarios classiques destinés à nuire sont notamment les suivants:

- Un ordinateur portable d'entreprise est corrompu avec un ver et infecte le réseau interne lorsqu'il se connecte
- L'équipement mobile d'un employé se connecte via un port Ethernet d'entreprise et infecte le réseau
- L'ordinateur portable infecté d'un prestataire contamine le réseau lorsqu'il dispose d'un accès non contrôlé

Et la conséquence logique de ces scénarios est l'indisponibilité du réseau. Dans le numéro du 12 janvier 2005 d'*ITWeek*, Martin Courtney cite une étude menée par le cabinet d'analyse Infonetics l'an dernier auprès de 80 grandes sociétés implantées aux États-Unis. Cette étude indique que ces grands comptes ont rapporté en moyenne 501 heures d'indisponibilité de leur réseau par an, ce qui leur coûte près de 4% de leur chiffre d'affaire, soit plusieurs millions de dollars. M. Courtney signale également qu'une autre enquête menée par le cabinet d'études Gartner rapporte que le coût horaire de l'indisponibilité du réseau pour les grandes entreprises s'élève à 42 000 dollars. «Une entreprise typique subit en moyenne 87 heures de temps d'arrêt par an, soit une perte totale supérieure à 3,6 millions de dollars.»²

Les mécanismes qui limitent la perte et les dommages liés à ces scénarios comprennent deux types de solution: les solutions **proactives** qui autorisent uniquement les connexions d'ordinateurs jugés fiables et les solutions **réactives** qui détectent les actions d'un ordinateur malveillant et l'isolent rapidement du reste du réseau. L'association des deux stratégies sera nécessaire pour satisfaire aux exigences face aux futures menaces.

Prévention d'intrusions par une analyse des postes

Une fois que des équipements d'extrémité infectés se connectent au réseau interne, les vers peuvent infecter des PC et serveurs Windows internes en l'espace de quelques minutes seulement. Puisqu'il y aura toujours des PC et des serveurs internes qui seront vulnérables, des stratégies de sécurité doivent être appliquées avant d'établir des connexions réseau.

Souvent appelée « technologie de mise en quarantaine », « analyse et blocage » ou « sandbox », la mise en quarantaine des postes est destinée à empêcher les systèmes corrompus d'accéder au réseau et à protéger les ressources de l'entreprise contre des systèmes connectés devenus corrompus.

Pour offrir une protection efficace, il analyse le périphérique qui tente de se connecter au réseau et le blocage de la connexion réseau si l'analyse découvre des patches manquants, des signatures antivirus périmées ou un firewall personnel mal configuré ou inexistant. Cependant, si une connexion réseau complète est déjà établie, l'analyse du système est déjà trop tard car les attaques depuis un système corrompu peuvent commencer au moment même de la connexion. Les technologies d'analyse et de blocage disponibles varieront selon que le système est administré ou non par l'entreprise et en fonction de la méthode de connexion. De nombreux scénarios doivent être explorés.

Le processus de mise en quarantaine évalue l'état de la sécurité d'un poste ou d'un utilisateur lorsqu'il connecte au réseau. Il supervise l'état de la sécurité des systèmes déjà connectés et déploie des stratégies de remédiation et d'accès au réseau en fonction de l'état du poste, de l'environnement de menaces et de l'identité des utilisateurs.

Les stratégies doivent définir les exigences de configuration de la sécurité, les règles d'identité et d'accès ainsi que les actions pour contrôler le réseau et la remédiation.

Les stratégies de protection peuvent concerner, mais sans s'y limiter, des niveaux de mise à jour logicielles, des signatures antivirales, des configurations spécifiques, des ports ouverts et fermés ainsi que des configurations de firewall.

La course à la création d'une norme de facto pour la gestion de l'accès au réseau

Comme rapporté par Roger A. Grimes dans le numéro du 5 septembre 2005 d'InfoWorld, l'épidémie désastreuse du ver Blaster en août 2003 « a confirmé que la protection de la passerelle en périphérie n'est pas suffisante et démontre une stratégie de sécurité défailante. » Et M. Grimes de continuer: « Depuis cet incident, l'adoption de firewalls personnels gérés de manière centrale est plus massive, les fournisseurs nous mijotent des initiatives à base de serveur pour durcir le cœur de réseau mou et élastique. » Selon Grimes, la bataille la plus intéressante concernant la défense des points d'extrémité et se déroule entre les initiatives Network Admission Control (NAC) de Cisco Systems et Network Access Protection (NAP) de Microsoft. Une troisième option a également fait son apparition: l'initiative Trusted Network Connect (TNC) de The Trusted Computing Group.³

« NAC et NAP n'en sont qu'à leur début. Nombre de fournisseurs prennent en charge ces deux premières plates-formes, mais la plupart des administrateurs réseau seront forcés de s'aligner dans un camp ou un autre pour faciliter l'administration centrale. Cisco et Microsoft mettent en avant l'interopérabilité de leurs initiatives. Les deux fournisseurs se sont même concédées mutuellement les licences de leur API respective, mais sans plus de détails. »

— Roger A. Grimes, *InfoWorld*

NAC de Cisco

Considéré comme « pionnière » et avant-gardiste, l'initiative Network Admission Control (NAC) de Cisco intègre la technologie de contrôle d'accès à ses gammes de produits d'accès au réseau. Pour ce faire, elle s'appuie sur l'infrastructure réseau afin d'appliquer la conformité aux stratégies de sécurité à tous les équipements cherchant à accéder aux ressources informatiques du réseau, ce qui limite les dommages liés aux virus et aux vers. L'initiative NAC peut également identifier les équipements non conformes et leur refuser l'accès, les mettre dans une zone de quarantaine ou leur fournir un accès limité aux ressources informatiques. NAC s'inscrit dans l'initiative Cisco de réseau à auto-défense (Cisco Self-Defending Network) dont l'objectif est d'accroître l'intelligence réseau pour permettre au réseau d'identifier et d'empêcher les menaces de sécurité et de s'y adapter, le tout de manière automatisée.

La phase 1 (diffusée en juin 2004) comprenait le support des routeurs d'agence plus récents de Cisco. Récemment diffusée, la phase 2 comprend le support des commutateurs Ethernet et des passerelles VPN. NAC exige l'agent CTA (Cisco Trust Agent) pour communiquer depuis le point d'extrémité. La fonction de base exige l'agent CSA (Cisco Security Agent) ou un agent tiers. Cisco a commencé à travailler avec des éditeurs de logiciels indépendants pour intégrer leurs fonctionnalités de base et d'atténuation des risques à NAC.

Dans le cadre de l'initiative NAC, Cisco partage des fonctionnalités technologiques avec des participants au programme tels que LANDesk. Les participants conçoivent et vendent leurs applications clientes et serveur ainsi que des services intégrant des fonctionnalités compatibles avec l'infrastructure NAC.

NAP de Microsoft

Actuellement dans une première phase de développement par rapport à l'initiative NAC de Cisco, Network Access Protection (NAP) de Microsoft est une plate-forme de déploiement de stratégies intégrée aux systèmes d'exploitation Microsoft Windows Vista et Windows Server "Longhorn". L'initiative NAP fournira les fonctionnalités de base, d'atténuation des risques et de contrôle d'accès au sein d'une infrastructure Microsoft. Une fois NAP disponible et le niveau système d'exploitation requis largement déployé, les fonctions de base et d'atténuation des risques de Cisco NAC seront disponibles sans qu'il soit nécessaire d'ajouter des agents supplémentaires.

NAP s'appuiera sur le protocole DHCP (Dynamic Host Configuration Protocol), 802.1x et IPsec (Internet Protocol Security) pour mettre les postes en quarantaine, même si l'intégration à l'initiative NAC de Cisco devrait fournir des options de contrôle alternatives. Microsoft diffusera NAP avec le serveur "Longhorn" en 2007.

Trusted Network Connect de TCG

The Trusted Computing Group (TCG) est une organisation sans but lucratif créée pour développer, définir et favoriser l'adoption de normes ouvertes pour des technologies de sécurité et informatiques matérielles de confiance. Le sous-groupe Trusted Network Connect de TCG a défini et mis au point une architecture ouverte et un ensemble croissant de normes pour garantir l'intégrité des points d'extrémité. Grâce à l'architecture TNC, les opérateurs de réseau peuvent appliquer des règles pour l'intégrité des points d'extrémité lors de ou après la connexion au réseau. Les normes sont conçues pour garantir une interopérabilité multiconstructeur sur un large éventail de points d'extrémité, de technologies réseau et de stratégies.

La mise en quarantaine réseau gagne du terrain

« 33% des entreprises nous déclarent qu'elles ont déjà recours à la mise en quarantaine réseau définie par Forrester comme la restriction dynamique de l'accès au réseau en fonction de la conformité à la stratégie de sécurité de l'entreprise. Ceci prouve que les entreprises sont en train d'intégrer la sécurité à des composants réseau tels que les commutateurs et les routeurs. 16% d'entreprises supplémentaires connaissant la mise en quarantaine réseau adopteront cette technologie au cours des 12 prochains mois, une fois que les solutions seront mûres et que des fournisseurs comme Cisco et Microsoft proposeront des offres plus complètes. Le décollage de la mise en quarantaine réseau indique une migration de la traditionnelle sécurité périmétrique basée sur des firewalls de réseau vers un environnement plus distribué mettant l'accent sur une authentification fiable associée à la sécurité des points d'extrémité. »⁴

— Natalie Lambert et Michael Speyer,
Forrester Research, Inc.

Fonctionnalités novatrices de LANDesk® Trusted Access™

Après avoir traité de la nécessité désormais impérieuse des solutions d'accès au réseau, intéressons-nous maintenant à LANDesk® Trusted Access™ et autres fonctionnalités de LANDesk® Security Suite.

Nouvelle technologie LANDesk d'analyse, de blocage et d'accès au réseau pour les entreprises qui utilisent LANDesk Security Suite, LANDesk Trusted Access vous permet de protéger votre réseau contre tout accès non autorisé et les menaces de sécurité externes telles que des équipements vulnérables ou des intrusions malveillantes pouvant infecter et endommager votre réseau. Les avantages de cette technologie sont: la réduction des risques d'indisponibilité des machines infectées et des intrusions malveillantes, un processus en matière d'application des stratégies de sécurité et de conformité et enfin la possibilité de sécuriser les utilisateurs nomades et invités.

Même si, de plus en plus, les entreprises bloquent les emails infectés et empêchent le téléchargement des codes malicieux avant que ces derniers ne puissent atteindre les postes de travail, l'un des moyens les plus classiques pour les virus de pénétrer le réseau est de transiter par les ordinateurs portables ayant séjourné en dehors de la zone de protection du réseau de l'entreprise. En effet, les utilisateurs d'ordinateurs portables qui consultent leur messagerie depuis un cybercafé ou qui téléchargent des logiciels via leur connexion Internet privée, ou depuis tout autre endroit n'ayant pas les mêmes moyens de contrôle que l'infrastructure de leur entreprise, peuvent être infectés. De retour au bureau, si ces utilisateurs sont autorisés à connecter leur ordinateur portable infecté au réseau d'entreprise, cette machine ouvre la voie à une infection qui se diffusera ensuite dans toute l'entreprise.

La menace venue de l'intérieur

Mais les utilisateurs nomades ou distants ne sont pas les seules sources de propagation d'infections dangereuses. En effet, tout équipement d'extrémité au sein du réseau qui n'est pas suffisamment protégé peut s'infecter et colporter malgré lui des codes malveillants. Autre menace, celle en provenance d'un partenaire commercial digne de confiance qui, en visite dans votre entreprise, souhaite pouvoir se connecter au réseau. Proposer ce service est certes un plus au niveau relationnel, mais cela peut tourner à la catastrophe pour le réseau si l'état de l'ordinateur portable de ce partenaire est incertain.

Lorsque ces ordinateurs ou d'autres tentent de se connecter au réseau de l'entreprise, LANDesk® Trusted Access™ les analyse pour vérifier leur intégrité et leur conformité à la stratégie de l'entreprise (patches à jour, configurations antivirus appropriées, menaces pour la configuration de la sécurité, etc.). Si un ordinateur s'avère non conforme ou infecté, la connexion au réseau lui est refusée. En outre, LANDesk® Security Suite peut automatiquement tenter de remédier à tout problème empêchant cette machine de se connecter. Une fois le problème résolu, l'ordinateur pourra se connecter.

Grâce à cette fonctionnalité d'analyse et de blocage, les entreprises ont la garantie que tout équipement d'extrémité qui tente de se connecter au réseau, qu'il appartienne à un utilisateur mobile, à un utilisateur interne, à un visiteur ou même à un entrepreneur externe, sera conforme à la stratégie de sécurité de l'entreprise avant qu'une connexion lui soit accordée. En effet, l'objectif est que cet équipement ne puisse pas constituer une menace d'infection pour le réseau.

LANDesk Trusted Access vous permet de définir des stratégies de sécurité personnalisées, d'analyser des équipements administrés et non administrés pour vérifier leur conformité aux stratégies. Cette solution permet en outre de refuser ou d'autoriser l'accès à vos ressources réseau critiques en fonction de la conformité de l'équipement à votre stratégie de sécurité.

Administrée de manière centralisée depuis une console unique et intégrée à LANDesk Security Suite, la fonctionnalité LANDesk Trusted Access vous permet de:

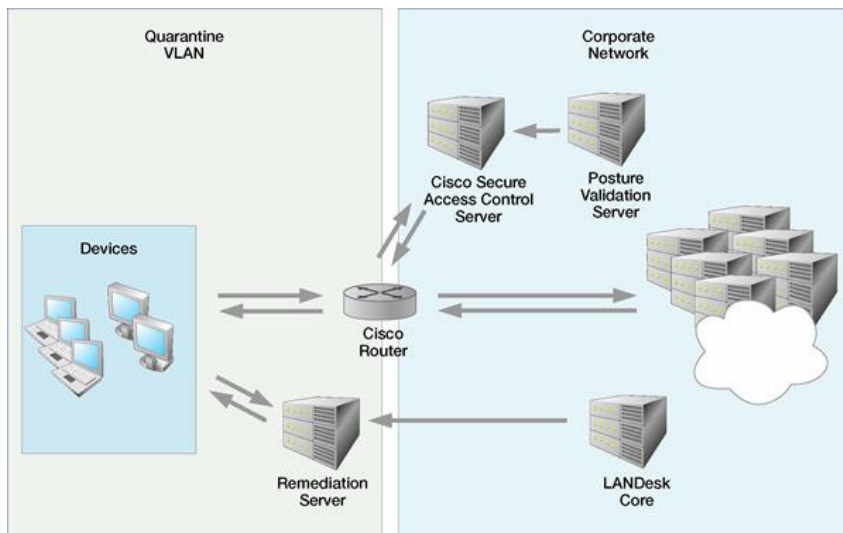
- Créer et imposer des stratégies de sécurité et de conformité
- Déployer une sécurité d'entreprise renforcée et permanente
- Évaluer les certificats de sécurité (état de santé) des équipements qui se connectent
- Analyser les nombreux types de sécurité – vulnérabilités, modification de la configuration initiale, antivirus, etc.
- Interdire l'accès au réseau aux systèmes infectés ou corrompus
- Mettre en quarantaine les équipements non conformes dans une zone sécurisée
- Réparer les équipements infectés pour les mettre en conformité
- Réduire le temps d'arrêt lié aux infections suite à des intrusions malveillantes
- Protéger votre réseau, vos systèmes, vos applications et vos données contre des menaces externes
- Étendre les technologies de sécurité et les normes existantes

Choix du support Cisco ou d'un matériel indépendant

LANDesk Trusted Access applique une sécurité périmétrique au niveau des points d'extrémité à l'aide de technologies et de systèmes de sécurité normalisés. Partenaire Cisco, LANDesk a annoncé le support de la stratégie de réseau à autodéfense Cisco Self-Defending, y compris l'initiative NAC. LANDesk est également un partenaire Microsoft prenant en charge l'initiative NAP. Qui plus est, LANDesk est un membre de The Trusted Computing Group qui préconise une approche de la sécurité des points d'extrémité basée sur une architecture ouverte et indépendante de tout constructeur.

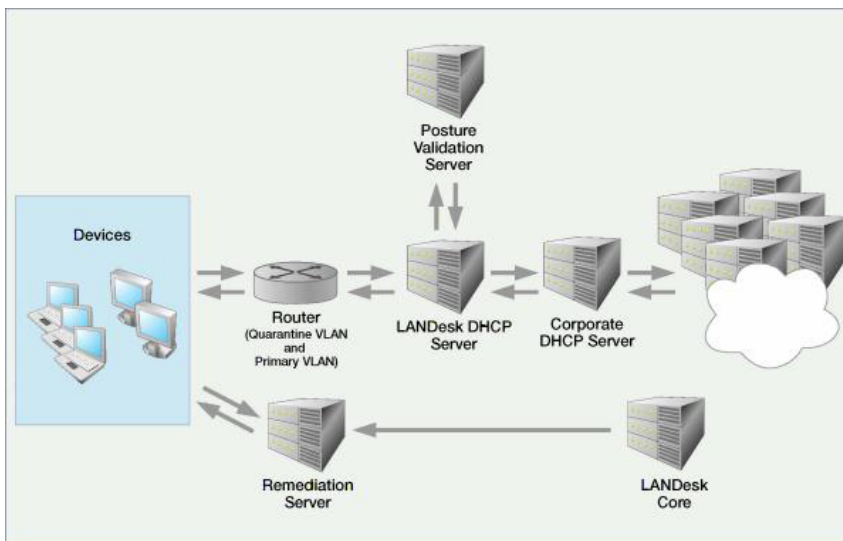
Actuellement, LANDesk propose aux entreprises deux options irrésistibles pour tirer parti de sa technologie de mise en quarantaine des postes. La première est une option compatible Cisco intégrée qui prend en charge et s'appuie sur l'initiative NAC. Cette solution est idéale pour les entreprises qui ont déployé une stratégie basée Cisco au sein de leur infrastructure réseau.

Composants Cisco NAC



La deuxième solution est la version DHCP de LANDesk® Trusted Access™. Indépendante au niveau matériel, cette option offre le même niveau de fonctionnalité que la solution basée sur Cisco. Elle tire cependant parti de pratiquement tout équipement serveur DHCP pour fournir ses fonctionnalités de prévention des intrusions.

Composants LANDesk DHCP



Protection préventive

Un élément majeur de la fonctionnalité de protection préemptive de LANDesk® Security Suite est sa capacité à superviser, analyser et appliquer des niveaux d'état pour les ressources antivirus, anti-spyware ainsi que les firewalls personnels. Cette solution procède à des analyses fréquentes pour détecter la non-conformité aux stratégies établies pour ces domaines puis utilise diverses méthodes pour restaurer et appliquer la conformité.

L'une des plus grandes menaces pour la capacité d'une entreprise à préserver son infrastructure informatique est la nature souvent complexe de ses efforts en matière de gestion de la sécurité. Lorsque les administrateurs informatiques doivent utiliser une batterie de consoles pour administrer leurs différentes solutions de sécurité, la confusion règne et les tâches de sécurité sont négligées. LANDesk® Security Suite unifie les efforts de gestion de la sécurité de l'entreprise grâce à une console d'administration centralisée à la fois puissante et souple. Par exemple, la console LANDesk Security Suite administre un large éventail de solutions antivirus tierces, notamment de:

- **Symantec**
- **Norton**
- **McAfee**
- **Trend-Micro**

Depuis cette console centralisée, les directeurs informatiques peuvent configurer les programmes antivirus de leur choix pour contrôler, prévenir et supprimer les virus connus. LANDesk Security Suite analyse également vos équipements d'extrémité pour vérifier que les programmes antivirus appropriés y sont bien, avec les moteurs d'analyse, les définitions de virus et les fichiers de configuration les plus récents. Si un équipement d'extrémité ne dispose pas des programmes et des fichiers appropriés ou les plus actualisés possibles, LANDesk Security Suite peut être configurée pour les télécharger automatiquement depuis le site de l'éditeur correspondant et les installer sur l'équipement en question.

Gestion proactive grâce à LANDesk® Management Gateway

Disponible dans les solutions de gestion LANDesk® 8.6, la nouvelle technologie LANDesk® Management Gateway vous permet d'atteindre et d'administrer de manière proactive des équipements non connectés au réseau local, sans qu'il soit nécessaire de faire d'ouvrir le firewall. S'appuyant sur une technologie brevetée, cette solution vous permet d'améliorer les processus métier, de protéger les données de votre entreprise et de vous conformer à la réglementation. Cette solution vous permet de :

- Protéger vos données métier et d'optimiser vos processus grâce à une gestion complète de la sécurité et de la configuration fournie par une solution simple et unifiée
- Prouver votre conformité aux normes et à la réglementation dans des environnements informatiques hétérogènes grâce au reporting complet de la gestion des biens et du contrôle de la configuration
- Protéger vos biens informatiques contre des attaques malveillantes en définissant et en appliquant une stratégie de sécurité
- Assurer un contrôle centralisé de la gestion au moyen de connexions directes via le réseau de votre entreprise et des connexions distantes via Internet

LANDesk Management Gateway sert de point d'interconnexion entre la console centrale et les équipements distants administrés via Internet. Et ce, que ces éléments se trouvent derrière des firewalls ou qu'ils s'appuient sur un serveur proxy pour accéder à Internet.

Extension du périmètre de préemption

LANDesk® Management Gateway et LANDesk® Trusted Access™ permettent d'étendre plus facilement aux utilisateurs distants les ressources de gestion de la sécurité préemptive fournies par LANDesk® Security Suite: gestion des patches, configuration du contrôle des connexions, fonctionnalités anti-spyware, analyse des menaces de sécurité pour les configurations, blocage des applications ainsi que le déploiement de fonctions anti-virus.

Que vos équipements d'extrémité soient installés à distance ou sur le réseau d'entreprise, LANDesk Trusted Access vous permet:

- d'interdire l'accès au réseau aux systèmes infectés ou non protégés
- de protéger les ressources de l'entreprise contre les systèmes connectés corrompus
- de définir des normes de conformité
- d'appliquer des stratégies de sécurité auxquelles les équipements d'extrémité doivent satisfaire avant de pénétrer sur le réseau d'entreprise

Conclusion

À l'heure où les fonctions métier sont de plus en plus orientées réseau et Internet, le réseau d'entreprise continue d'être un composant opérationnel critique pour l'entreprise. Et plus la valeur métier du réseau continuera d'augmenter, plus les attaques à base de vers et de virus tenteront de perturber l'entreprise en endommageant son réseau, avec pour corollaire des pannes système et de pertes d'opportunités, donc de revenus.

LANDesk® Trusted Access™ et d'autres fonctionnalités de LANDesk® Security Suite fournissent des niveaux éprouvés de protection de votre réseau. Vous empêcherez ainsi des équipements vulnérables ou corrompus d'accéder au réseau et protégerez les ressources critiques de votre réseau contre les systèmes connectés corrompus.

Références

¹ « Surviving the Endpoint Security Policy Enforcement Melee, » Jim Slaby, analyste en chef, entité Solutions & Services de sécurité au Yankee Group, 11 mai 2005

² « Firms Fail to Count Costs of Downtime, » Martin Courtney, *IT Week*, 12 janvier 2005

³ « NAC vs. NAP: Network access management locks out untrusted end points; Cisco and Microsoft are duking it out over who gets the keys, » Roger A. Grimes, *InfoWorld*, 5 septembre 2005

⁴ « The State of Security in SMBs and Enterprises, » Natalie Lambert et Michael Speyer, Forrester Research, Inc., 21 septembre 2005