GESTION DES SYSTÈMES : LE GUIDE DES BONNES PRATIQUES

SOMMAIRE

Page

1. INTRODUCTION 2

2. UNE DIVERSITÉ CROISSANTE 3

3. CENTRALISATION, AUTOMATISATION, CONTRÔLE 3

4. CONTRÔLE ET MISE EN ŒUVRE EFFICACE DES IMAGES/DU PROVISIONNEMENT 4

5. INSTALLATION ET DÉPLOIEMENT DES LOGICIELS 5

6. GESTION ET CONTRÔLE EFFICACES DES LICENCES 6

7. ANALYSE AVANCÉE DES VULNÉRABILITÉS ET GESTION DES CORRECTIFS 7

8. CONTRÔLE D'ACCÈS AU RÉSEAU (NAC) 8

9. GESTION CENTRALISÉE DES CONFIGURATIONS ET DES CORRECTIFS POUR UNE MEILLEURE EFFICACITÉ 9

10. CONCLUSION 9

COMPOSANTS ESSENTIELS DE LA SÉCURITÉ DES TERMINAUX.

1. INTRODUCTION

« Être plus performant tout en faisant appel à des ressources plus limitées ». Telle est la devise que les entreprises ont adoptée depuis quelques années, devise que les professionnels de l'informatique connaissent déjà fort bien. Le monde de l'entreprise a toujours cherché à exploiter au maximum les ressources informatiques au coût le plus bas possible. Or, le véritable enjeu des services informatiques consiste actuellement à s'adapter à un contexte toujours plus complexe en s'appuyant sur des ressources moindres.

Dans son rapport intitulé Global State of Information Security (Bilan sur la sécurité de l'information)[1], PriceWaterhouseCoopers indique que les risques liés à la sécurité informatique sont plus importants que jamais, avec l'apparition de nouvelles règles et l'entrée en lice de nouveaux protagonistes hautement qualifiés. Pour remporter cette bataille, les entreprises doivent se préparer à un challenge d'un nouveau genre nécessitant des compétences et une stratégie avancées.

De plus, une enquête récente menée par Kaspersky Lab[2] a révélé l'existence d'un contexte de sécurité de plus en plus chaotique dans lequel plus de 40 % des entreprises ne se sentent pas préparées aux menaces qui les entourent. Ce n'est pas une surprise : Kaspersky Lab enregistre en moyenne 125 000 nouvelles menaces par jour. 58 % des utilisateurs interrogés évoquent un manque de ressources pour assurer la sécurité informatique dans au moins l'un des domaines suivants : personnel, systèmes ou connaissances.

1 Référence : rapport de PriceWaterhouseCoopers intitulé Global State of Information Security (Bilan sur la sécurité de l'information) publié en 2013
2 Source : rapport 2012 de Kaspersky sur les risques informatiques mondiaux

2. UNE DIVERSITÉ CROISSANTE

De plus, il ne s'agit plus simplement des menaces extérieures. La diversité croissante des plates-formes, périphériques, logiciels et applications complique la tâche des responsables informatiques et génère complexité et épuisement des ressources. Par exemple :

- Périphériques multiples
- Solutions de fournisseurs multiples
- Consoles d'administration multiples
- Images de systèmes d'exploitation multiples
- Périphériques réseau multiples
- Politiques multiples

Une telle complexité compromet la sécurité, l'efficacité et la croissance. Elle est à l'origine d'erreurs et limite votre capacité à gérer le changement. Les professionnels de l'informatique sont tout à fait conscients de ces problématiques. Mais quelle solution adopter pour atténuer ces problèmes sans pour autant restreindre les besoins des utilisateurs finaux ou surcharger des ressources déjà bien sollicitées ?

Une **gestion efficace des systèmes** peut contribuer à l'adoption des meilleures pratiques visant à optimiser les ressources informatiques tout en imposant un niveau de sécurité capable de faire face à l'évolution constante des menaces. Les processus manuels fastidieux et le manque de visibilité sur votre réseau constituent deux des plus importants défis auxquels le responsable informatique est confronté aujourd'hui.

De la **gestion des licences**, à **l'installation des logiciels, l'analyse automatisée des vulnérabilités en passant par la gestion avancée des correctifs, la création/le déploiement d'images des systèmes d'exploitation** et **le contrôle d'accès au réseau (NAC)**, chaque heure consacrée à la maintenance et à la surveillance est une heure que vous pourriez passer à développer de nouvelles idées ou à soutenir de nouvelles initiatives. Ce guide a été créé précisément pour vous aider à accomplir ces opérations.

3. CENTRALISATION, AUTOMATISATION, CONTRÔLE

Pour garantir des performances informatiques optimales, réduire les coûts, améliorer les niveaux de service et renforcer l'agilité, toutes les entreprises sont tenues de prendre certaines mesures essentielles :

- Uniformisation de la stratégie en matière de postes de travail et d'ordinateurs portables et réduction des images au minimum ;
- Gestion centralisée des paramètres et des configurations des PC, ordinateurs portables et périphériques nomades ;
- Mise en œuvre et gestion d'outils de sécurité complets ;
- Automatisation de la distribution logicielle, de la gestion des correctifs et de l'analyse des vulnérabilités, ainsi que d'autres tâches de routine ;
- Optimisation du budget et de l'utilisation des logiciels et du matériel ;
- Mise en œuvre d'une procédure de contrôle d'accès au réseau efficace et facile à gérer.

L'automatisation des principales tâches récurrentes (de la sécurité au dépannage) permet aux administrateurs de passer d'une approche de gestion des urgences à une approche stratégique qui intègre la prise en charge des besoins en phase avec les politiques informatiques. L'automatisation peut contribuer à réduire les erreurs souvent liées à l'exécution de processus manuels dans des systèmes complexes.

4. CONTRÔLE ET MISE EN ŒUVRE EFFICACE DES IMAGES/DU PROVISIONNEMENT

Chaque année, vous déployez du matériel neuf et de nouvelles applications et vous mettez sans cesse à niveau des logiciels, des systèmes d'exploitation. Sans parler des correctifs et des mises à jour. Il s'agit d'un processus fastidieux, onéreux et complexe en raison de l'augmentation des inventaires.

La préparation et la gestion d'une « Golden Image », à savoir un modèle principal entièrement optimisé (ou un clone en quelque sorte) d'un poste de travail complet, permettant un gain de temps et de ressources considérable. Ce modèle d'installation idéal est stocké dans un inventaire spécifique sur votre réseau et peut être déployé selon vos besoins. Les entreprises qui comptent migrer vers un nouveau système d'exploitation peuvent automatiser le contrôle des images/du provisionnement, l'inventaire et le déploiement. L'avantage réel de cette solution ? Les administrateurs peuvent déployer un nouveau système d'exploitation en dehors des heures ouvrées grâce à la technologie BootOnLAN, qui permet de gagner davantage de temps et de perturber au minimum l'activité.

Une gestion efficace du déploiement des images/des services de provisionnement garantit une mise en œuvre des systèmes d'exploitation avec des paramètres de sécurité optimaux. Mais n'oubliez pas de veiller à la sécurité des images elles-mêmes. Il est de rigueur de sécuriser et de contrôler l'accès à l'ensemble des images en s'appuyant sur les mesures suivantes :

- Mots de passe complexes ;
- Protection des certificats d'authentification client ;
- Contrôle des accès afin de protéger l'ordinateur « de référence » utilisé pour capturer le système d'exploitation que vous utilisez en vue de créer la « Golden Image ». Ceci empêche les logiciels malveillants de pénétrer, par inadvertance, dans l'image ;
- S'assurer que l'image est enregistrée dans un emplacement sécurisé afin d'éviter toute forme d'infection ;
- Gestion des correctifs et des mises à jour de sécurité sur le système de référence afin de garantir la sécurité optimale des nouveaux systèmes déployés.

Si votre entreprise envisage de migrer vers Windows 8, une gestion efficace des images/du provisionnement vous permettra d'uniformiser le système d'exploitation utilisé sur l'ensemble des périphériques de votre réseau. Choisissez une solution capable d'automatiser et de gérer les images de manière centralisée. Gagnez en confort en optant pour une solution qui enregistre automatiquement les données des utilisateurs.

5. INSTALLATION ET DÉPLOIEMENT DES LOGICIELS

Mises à niveau des logiciels. Nouveaux logiciels. Nouvelles versions des logiciels en cours d'utilisation. Impossible de procéder à une mise à niveau manuelle de chacune des machines de l'entreprise ; il ne vous resterait plus de temps pour faire autre chose. Le déploiement logiciel peut être automatisé et optimisé afin de garantir un impact minimal sur votre réseau. Et, grâce à une technologie de « déploiement silencieux », le déploiement est totalement transparent pour les utilisateurs.

Quelques conseils :

- **Envisagez des options de déploiement ouvertes :** outre les progiciels MSI standard, optez pour une solution qui prend en charge d'autres types de fichiers exécutables, notamment les formats exe, bat ou cmd.

- **Faites preuve de flexibilité en matière de déploiement :** si vous optez pour des solutions permettant des déploiements à la demande et programmés, vous gagnerez en souplesse. Les déploiements programmés sont particulièrement utiles dans des scénarios de déploiement importants. Il vous suffit de les réaliser en dehors des heures de bureau pour minimiser les perturbations réseau.

- **Modification du programme d'installation :** cette fonctionnalité offre davantage de flexibilité puisqu'elle vous permet de définir des paramètres d'installation afin de garantir la compatibilité avec vos politiques.

- **Gestion de l'installation et du trafic à distance :** si vous prenez en charge des sites distants, optez pour une solution capable de gérer un trafic plus important en affectant un agent de mise à jour à un poste de travail déterminé. Les programmes d'installation seront téléchargés par cette machine en premier lieu, avant d'être distribués vers d'autres postes de travail locaux. Ceci permet de limiter la charge réseau et de réduire considérablement l'utilisation de la connexion Internet.

- **Vous pouvez atténuer davantage cette charge en vous appuyant sur la technologie de diffusion multicast** qui permet une diffusion depuis une source unique vers un groupe de machines ou depuis plusieurs sources vers un groupe de machines.

- **Dépannage à distance :** vous n'aurez plus à subir d'appels téléphoniques frustrants avec les utilisateurs. Le dépannage à distance, qui permet de résoudre les problèmes rapidement et directement, permet de gagner du temps et d'être plus efficace.

Le déploiement et la mise à niveau des logiciels représentent une activité banale pour les administrateurs informatiques. En automatisant et en optimisant cette activité, vous êtes certain que les meilleures pratiques recommandées seront suivies par défaut. Dans des scénarios multi-sites ou multi-systèmes, la maîtrise des déploiements logiciels peut permettre de réduire la complexité et les erreurs liées à des processus manuels répétitifs.

6. GESTION ET CONTRÔLE EFFICACES DES LICENCES

La capacité à gérer et à contrôler les licences logicielles dans l'entreprise constitue, pour les professionnels de l'informatique, l'une des mesures les plus simples pour optimiser les coûts.

Outre la possibilité de réduire les coûts en supprimant les dépenses excessives dans des logiciels inutiles, un meilleur contrôle des licences favorise une stratégie de sécurité plus efficace. Si vous avez précisément identifié le logiciel et la personne qui l'utilise sur votre réseau, il est plus facile d'appliquer vos politiques.

En matière de gestion des licences logicielles et matérielles, il est recommandé de disposer d'une visibilité totale sur chaque logiciel/matériel exécuté sur votre réseau. La technologie de détection automatique des périphériques agit dans ce sens et vous garantit le respect de toutes les obligations liées aux licences.

Autres mesures possibles :

- **Inventaire logiciel :** automatisez le processus d'inventaire de tous les logiciels utilisés sur votre réseau et bénéficiez d'une visibilité complète et d'un contrôle total. Grâce à cette liste, les administrateurs peuvent surveiller l'usage d'un logiciel interdit/sans licence et en informer les utilisateurs, voire bloquer l'accès aux applications non recommandées, le cas échéant.

- **Planification des licences :** après avoir dressé un inventaire, il est plus facile de contrôler les licences en fonction des besoins des services. Vous pouvez, par exemple, identifier que des utilisateurs du service comptabilité sont titulaires de licences inutiles pour des logiciels bureautiques. Ces licences peuvent être redéployées ou supprimées pour réduire les coûts. En dressant un état des lieux précis des licences utilisées dans votre entreprise, vous serez également à même de veiller à leur mise à jour. Vous pouvez, de surcroît, procéder à un suivi automatique des infractions.

- **Suivi des inventaires matériels et des périphériques :** tout comme pour les logiciels, cet inventaire matériel vous offre un état des lieux précis des différents périphériques utilisés sur votre réseau. Automatisez le processus de détection et de notification du matériel neuf pour disposer de données actualisées, surveillez les changements et archivez les périphériques qui ne sont pas utilisés.

- **Rapports :** l'édition de rapports centralisés est une source d'informations exhaustives sur chaque logiciel et chaque équipement matériel utilisés sur votre réseau et offre un historique d'utilisation. Les données issues de ces rapports vous permettront de contrôler l'utilisation au sein des différents groupes et à tous les niveaux de l'entreprise.

Le contrôle des licences est un processus fastidieux et souvent complexe. Vous pouvez automatiser cette tâche pour vous libérer du temps, mais également pour veiller au respect des meilleures pratiques, notamment dans les domaines suivants : **conformité, gestion économique des logiciels et du matériel et visibilité totale sur l'activité de votre réseau**. Un effort mineur pour un bénéfice majeur. Alors, qu'attendez-vous ?

7. ANALYSE AVANCÉE DES VULNÉRABILITÉS ET GESTION DES CORRECTIFS

Les services informatiques sont confrontés à des tâches importantes, difficiles et qui requièrent la mobilisation de ressources considérables. La gestion et l'administration des mises à jour logicielles, ainsi que la surveillance continue des vulnérabilités potentielles, sont l'une de ces tâches.

Dans un environnement constitué de menaces en constante évolution au sein duquel les criminels analysent sans cesse les systèmes pour détecter tout signe de faiblesse, les administrateurs informatiques doivent impérativement identifier et combler les failles de sécurité avant qu'elles ne soient exploitées.

La fonction d'analyse des vulnérabilités exécute cette tâche à votre place en analysant les périphériques et les logiciels de votre réseau, tel que le ferait un criminel qui chercherait à identifier les points faibles dont il pourrait tirer profit. Une fois les vulnérabilités localisées, l'outil de gestion des correctifs est en mesure de combler ces lacunes en installant les mises à jour requises ou en réparant les logiciels sur toutes les machines installées sur votre réseau.

La mise en œuvre d'une analyse des vulnérabilités associée à une stratégie de gestion des correctifs efficace peut vous permettre de garder une longueur d'avance sur les pirates informatiques. Marche à suivre :

- **Se tenir informé :** des logiciels obsolètes créent des vulnérabilités au sein de l'entreprise, qu'ils soient installés sur vos serveurs ou sur un poste de travail. Une analyse des vulnérabilités automatisée et régulière vous permet de rester informé des failles et d'automatiser ainsi l'application des correctifs.
- **Automatisation :** gestion efficace des correctifs pour une fiabilité et des performances informatiques renforcées. En automatisant le déploiement des mises à jour logicielles et les tâches administratives associées, vous pouvez réduire les temps d'arrêt liés au déploiement des correctifs, aux audits et à la restauration.
- **Restauration :** les mises à jour et les installations ne fonctionnent pas toujours parfaitement. Les correctifs peuvent parfois générer une instabilité ou être incompatibles avec d'autres logiciels ou pilotes installés sur vos machines. L'adoption d'une solution avec fonction d'image/de provisionnement intégrée, qui offre la possibilité d'un retour à un état de fonctionnement optimal du système, s'avère toujours la méthode la plus simple.
- **Visibilité complète :** automatisez l'analyse et bénéficiez d'une visibilité totale sur l'état actuel des correctifs et des mises à jour sur toutes les machines.
- **Hiérarchisation :** en comparant les résultats de vos analyses avec différentes bases de données des vulnérabilités, vous cernez les risques associés aux vulnérabilités, quelles qu'elles soient. Au vu de ces informations, vous êtes en mesure de définir un ordre de priorité dans l'application des correctifs, le déploiement des correctifs qui ne revêtent aucun caractère d'urgence en dehors des heures ouvrées et la répartition de la charge sur votre réseau.
- **Rapports :** une stratégie de gestion de la sécurité et des risques repose essentiellement sur des données précises, actualisées et détaillées. L'exécution de rapports basés sur les analyses vous permet de bénéficier d'informations encore plus précises grâce auxquelles vous pouvez examiner et vous rendre compte des failles potentielles, identifier et suivre les modifications tout en obtenant des rapports détaillés sur l'état des correctifs pour chaque périphérique et système de votre réseau.

Les attaques ciblées et automatisées, les menaces persistantes avancées et les vulnérabilités « zero-day » réduisent considérablement le délai entre la détection des vulnérabilités et le développement des failles d'exploitation. En automatisant et en planifiant les analyses et la mise en œuvre des correctifs, les administrateurs informatiques peuvent rationaliser la gestion des correctifs et des processus d'analyse des vulnérabilités sans nuire à leur efficacité.

8. CONTRÔLE D'ACCÈS AU RÉSEAU (NAC)

Vous contrôlez les images/le provisionnement et les licences, vous avez automatisé l'installation des logiciels et avez mis en place un système de gestion avancée des analyses et des correctifs. Vous pouvez à présent appliquer des niveaux de connaissances et de contrôle similaires à votre réseau, aux périphériques et aux machines qui s'y connectent.

Le contrôle d'accès au réseau permet aux administrateurs informatiques d'appliquer des politiques de sécurité visant à refuser ou à limiter l'accès au réseau en se basant sur le respect de ces politiques, et ce quel que soit le périphérique. En résumé, le contrôle d'accès au réseau offre aux administrateurs la possibilité de définir les conditions d'utilisation de leur réseau, y compris pour les périphériques des visiteurs. Pour les entreprises qui prennent en charge les appareils personnels ou dont le nombre d'employés nomades ne cesse d'augmenter, la solution de contrôle d'accès au réseau garantit que tous les périphériques (ordinateurs portables, PC et smartphones) utilisent des versions actualisées et sécurisées des applications et des logiciels que vous avez spécifiés.

Le contrôle d'accès au réseau prend en charge les stratégies et politiques de sécurité existantes tout en imposant les meilleures pratiques, et notamment :

- Empêcher les périphériques non autorisés d'accéder au réseau ;
- Détecter et identifier les nouveaux périphériques qui se connectent au réseau ;
- Imposer à tous les périphériques, y compris aux systèmes des visiteurs, le respect des exigences de sécurité que vous avez spécifiées ;
- Détection et réparation des vulnérabilités des terminaux ;
- Aperçu de la conformité aux politiques de sécurité et rapports.

Avant de mettre en œuvre une procédure de contrôle d'accès au réseau, il est essentiel de déterminer précisément l'objectif à atteindre (ex. : autoriser les visiteurs à utiliser Internet dans un espace commun sur votre site, mais bloquer l'accès aux réseaux internes). Vous souhaitez probablement veiller à ce que tous les ordinateurs portables des visiteurs soient protégés contre les programmes malveillants et bénéficient d'un certain niveau de sécurité.

Voici quelques questions qu'il convient de se poser :

- Qui est autorisé à se connecter au réseau ?
- À quels services et à quelles ressources les utilisateurs sont-ils autorisés à accéder ?
- Quand cet accès doit-il être accordé ?
- Depuis quels sites les utilisateurs sont-ils autorisés à se connecter ?
- Certains types de groupes d'utilisateurs doivent-ils être limités à certains types de ressources ou disposer d'un accès restreint à des heures particulières ?

Un contrôle d'accès au réseau efficace doit reposer sur un dispositif de détection automatique des périphériques, qui permet de distinguer les périphériques appartenant à l'entreprise de ceux des visiteurs et d'appliquer des politiques et des accès en conséquence. Gagnez du temps et épargnez vos efforts en automatisant les accès. Vous pouvez ainsi créer une politique de gestion des accès et l'appliquer à l'ensemble des périphériques.

Il est possible de renforcer la sécurité sur tous les périphériques des visiteurs à l'aide d'un « portail captif ». Pour ce faire, tous les périphériques des visiteurs sont dirigés automatiquement vers ce portail spécifique. Un identifiant de connexion et un mot de passe sont attribués aux visiteurs qui, une fois identifiés, peuvent accéder à Internet et à certaines ressources de l'entreprise prédéfinies, s'ils y ont été autorisés.

9. GESTION CENTRALISÉE DES CONFIGURATIONS ET DES CORRECTIFS POUR UNE MEILLEURE EFFICACITÉ

Les professionnels de l'informatique bataillent pour gagner en productivité tout en sollicitant des ressources et des budgets plus limités, au risque de perdre toute visibilité et tout contrôle sur les réseaux de l'entreprise. Ils doivent être attentifs aux problèmes urgents, souvent au détriment des tâches essentielles, certes ordinaires.

En centralisant et en automatisant de nombreuses tâches de configuration et de gestion indispensables, les administrateurs informatiques peuvent gagner du temps et réaliser des économies. Une gestion efficace des systèmes régie par des outils centralisés de gestion des configurations et des correctifs favorise nombre de meilleures pratiques visant à optimiser les ressources informatiques tout en appliquant les politiques spécifiques à votre entreprise.

10. CONCLUSION

Les entreprises ont besoin de compter sur des technologies intelligentes en matière de sécurité dans le but de protéger leurs données, ainsi que sur des outils informatiques à la fois intuitifs et simples d'utilisation, garants de l'efficacité de leurs opérations. Les 2 500 collaborateurs de Kaspersky Lab ont à cœur de répondre aux besoins de plus de 300 millions d'utilisateurs dont ils assurent la protection et 50 000 nouveaux utilisateurs qui s'ajoutent chaque jour.

Kaspersky Systems Management est une composante de Kaspersky Endpoint Security for Business. Outils primés en matière de protection anti-malware, d'application des politiques informatiques, de gestion centralisée et de protection basée sur le cloud : votre entreprise dispose ainsi des solutions de sécurité Kaspersky parfaitement adaptés à ses besoins.

Contactez votre revendeur informatique pour découvrir comment Kaspersky peut sécuriser votre réseau informatique et bien davantage !

IDENTIFIER. CONTRÔLER. PROTÉGER.

Avec Kaspersky, maintenant, c'est possible.
kaspersky.com/fr/business-security

Be Ready for What's Next

Kaspersky Lab ZAO, Moscou, Russie
www.kaspersky.com/fr