KASPERSKY lab

GUIDE DES BONNES PRATIQUES

Gestion des systèmes

www.kaspersky.fr

VOTRE GUIDE DES BONNES PRATIQUES EN MATIÈRE DE GESTION DES SYSTÈMES.

Renforcez la sécurité et réduisez la complexité de votre environnement grâce à des outils d'administration informatique centralisés.

Les vulnérabilités non corrigées dans les applications largement utilisées représentent l'une des plus grandes menaces pour la sécurité informatique des entreprises. Ce risque est aggravé par l'accroissement de la complexité informatique. Si vous ne savez pas ce que vous avez, comment pouvez-vous le sécuriser ? Le présent Guide des bonnes pratiques vous en dit plus...

La diversité croissante des plateformes, appareils, logiciels et applications complique la tâche des responsables informatiques et est source de complexité et d'épuisement des ressources. Appareils et logiciels ne sont pas les seuls à se multiplier ; Kaspersky Lab détecte 350 000 nouvelles menaces chaque jour, dont un grand nombre sont spécifiquement conçues pour exploiter les vulnérabilités des applications professionnelles les plus courantes, pour accéder à des données sensibles, voler de l'argent ou bloquer les systèmes jusqu'à ce qu'une rançon soit versée.

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. Une gestion efficace des systèmes peut contribuer grandement à l'adoption des meilleures pratiques visant à optimiser les ressources informatiques, tout en soutenant une stratégie de sécurité multiniveaux capable de faire face à l'évolution constante des menaces. Telle est la marche à suivre :

1. CENTRALISATION, AUTOMATISATION, CONTRÔLE

Commencez par prendre certaines mesures essentielles pour garantir des performances informatiques optimales, réduire les coûts, améliorer les niveaux de service et renforcer l'agilité.

- Uniformisez la stratégie en matière de postes de travail et d'ordinateurs portables et réduisez les images au minimum.
- Adoptez une gestion centralisée des paramètres et des configurations des PC, ordinateurs portables et appareils mobiles.
- Mettez en œuvre et gérez des outils de sécurité complets.
- Automatisez les inventaires matériels et logiciels, la distribution des logiciels, l'analyse des vulnérabilités, la gestion des correctifs et autres tâches de routine.
- Activez le dépannage et l'installation de logiciels à distance, y compris dans les bureaux distants.
- Mettez en œuvre le contrôle des accès basé sur les rôles, personnalisez les affichages de la console centralisée en fonction des rôles et des droits.
- Pour les grandes entreprises, l'intégration avec les systèmes SIEM contribue à réduire la charge de travail de l'administrateur et les outils tout en simplifiant l'établissement des rapports.

L'automatisation des principales tâches de routine (de la sécurité au dépannage) permet de passer d'une situation 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.

2. CONTRÔLE ET MISE EN ŒUVRE EFFICACES DES IMAGES

Chaque année, de nouveaux matériels et applications sont déployés, ainsi que des mises à niveau régulières des logiciels, des systèmes d'exploitation et des correctifs. 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, permettent des gains de temps et de ressources considérables. Ce modèle d'installation « idéal » est stocké dans un inventaire spécifique sur le réseau et peut être déployé au gré des besoins. Les entreprises migrant vers un nouveau système d'exploitation peuvent automatiser le contrôle des images, l'inventaire et le déploiement. Cette automatisation a l'avantage de permettre les déploiements en dehors des heures de travail grâce à la technologie Wake-on-LAN, ainsi que de réduire le temps de travail et les perturbations pour les utilisateurs finaux.

Un déploiement efficace des images garantit une mise en œuvre des systèmes d'exploitation avec des paramètres de sécurité optimaux. Mais n'oubliez pas la sécurité des images elles-mêmes. Il est de rigueur de sécuriser et de contrôler l'accès à l'ensemble des images, notamment par les moyens suivants :

- Mots de passe difficiles à détourner
- Protection des certificats d'authentification client
- Contrôles d'accès pour protéger l'ordinateur de « référence » utilisé pour capturer le système d'exploitation utilisé pour la « Golden Image », de manière à empêcher tout logiciel malveillant d'être inclus par inadvertance dans l'image
- S'assurer que l'image est enregistrée dans un emplacement sécurisé où elle ne peut être infectée
- Gérer les correctifs et mises à jour de sécurité sur le système de référence afin de garantir la sécurité optimale de tous les nouveaux systèmes mis en œuvre

Une gestion d'image efficace vous permet d'uniformiser votre système d'exploitation sur tous les appareils de votre réseau. Choisissez une solution qui permet l'automatisation et la gestion centralisée des images. Gagnez en confort en optant pour une solution qui enregistre automatiquement les données des utilisateurs finaux.

Pour plus de contrôle et de flexibilité, recherchez une solution qui permet aux images de systèmes d'exploitation d'être modifiées après leur création. Prise en charge UEFI, possibilité de créer un disque flash de démarrage avec Windows PE et possibilité d'importer une image de système d'exploitation à partir d'un package de distribution sont autant de fonctionnalités qui amélioreront encore la convivialité et l'efficacité.

3. OPTIMISATION DE L'INSTALLATION ET DU DÉPLOIEMENT DES LOGICIELS

Mises à niveau des logiciels. Nouveaux logiciels. Nouvelles versions des logiciels actuels. La mise à niveau manuelle de chaque machine dans l'entreprise ne laisserait pas de temps pour effectuer d'autres tâches. Le déploiement de logiciels peut être automatisé et optimisé pour assurer un impact minimum sur le réseau, rendant cette opération totalement transparente pour les utilisateurs finaux. Voici quelques conseils concernant les bonnes pratiques à mettre en place :

- Laissez les options de déploiement ouvertes en sélectionnant une solution qui, en plus des packages MSI standard, prend en charge d'autres types de fichiers exécutables, tels que exe, bat ou cmd.
- Faites preuve de flexibilité en matière de déploiement : les options permettant aussi bien des déploiements programmés et à la demande offrent une plus grande souplesse. Les déploiements programmés sont particulièrement utiles dans des scénarios de déploiement importants ; déployer en dehors des heures de bureau minimise les perturbations. Kaspersky Systems Management permet l'installation automatique de plus de 100 applications populaires identifiées via Kaspersky Security Network. Elles peuvent être installées en dehors des heures de bureau, si nécessaire.
- Choisissez une solution qui permet les déploiements à distance à partir d'une console unique. Trafic réduit vers les sites distants grâce à la technologie Multicast pour la distribution logicielle en local.
- La fonctionnalité de modification du programme d'installation offre davantage de flexibilité puisqu'elle vous permet de définir des paramètres d'installation afin de garantir la compatibilité avec vos politiques.
- Choisissez une solution permettant le dépannage à distance pour ne plus subir d'échanges téléphoniques pénibles avec les utilisateurs finaux. Le dépannage à distance, qui permet de résoudre les problèmes rapidement et directement, vous fait gagner du temps tout en vous facilitant la tâche. Les autorisations utilisateur et les journaux de session/vérifications ajoutent une couche de sécurité supplémentaire pour les sessions à distance.

L'automatisation et l'optimisation du déploiement et des mises à niveau de logiciels vous permettent d'appliquer par défaut les directives des bonnes pratiques dans votre entreprise. Dans des environnements multi-sites ou multi-systèmes, la maîtrise des déploiements logiciels contribue à réduire la complexité et les erreurs liées aux processus manuels répétitifs.

4. PRISE DE CONTRÔLE DES RESSOURCES

Savoir exactement quels appareils et applications sont utilisés sur votre réseau est une composante clé d'une sécurité informatique efficace. Savoir quels domaines ont besoin d'attention l'est également.

La meilleure pratique consiste à avoir une visibilité complète sur chaque logiciel et matériel fonctionnant sur votre réseau. La technologie de détection automatique des appareils agit dans ce sens et vous garantit que toutes les obligations sont respectées. Les autres mesures incluent notamment ce qui suit :

- **Inventaire des logiciels** : automatisez la compilation d'inventaire et obtenez une visibilité et un contrôle complets. Cette liste permet aux administrateurs de surveiller l'usage de tout logiciel non autorisé/sans licence et d'en informer les utilisateurs finaux, voire de bloquer l'accès aux applications non recommandées si nécessaire. La gestion et le contrôle des licences de logiciels au sein de l'entreprise constituent l'un des moyens les plus simples de réduire les coûts en éliminant les dépenses liées à des logiciels inutiles.

- **Inventaire matériel et suivi des appareils** : offre une vue complète de tous les appareils en cours d'utilisation sur le réseau. Automatisez le processus de détection et de notification du matériel neuf pour disposer de données actualisées, surveillez les changements et archivez les appareils qui ne sont pas utilisés. Le contrôle d'accès au réseau (NAC) permet l'ajout des appareils de visiteurs sur le réseau en toute sécurité, leur blocage s'ils ne satisfont pas aux exigences de sécurité ou l'application de politiques différentes à ces appareils.

- **Planification des licences** : une fois l'inventaire dressé, il est plus facile de contrôler l'utilisation des licences en fonction des besoins des services. Vous pouvez par exemple déterminer que des utilisateurs du service de comptabilité disposent de licences de logiciels de conception graphique inutiles, qui pourraient être redéployées ou progressivement éliminées. En outre, disposer d'une vision claire des licences permet une gestion en phase avec la situation actuelle.

- **Rapports** : l'édition de rapports centralisés est une source d'informations exhaustives sur chaque logiciel et chaque matériel présent sur le réseau ; elle offre également un historique d'utilisation. Les connaissances tirées de ces rapports permettent de contrôler l'usage au sein des groupes à tous les niveaux.

Le contrôle des licences est un processus fastidieux et complexe. Vous pouvez automatiser cette tâche pour non seulement vous libérer du temps, mais également pour veiller au respect des bonnes 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.

5. ÉVALUATION DES VULNÉRABILITÉS ET GESTION DES CORRECTIFS AVANCÉES

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, en font partie.

Face aux menaces ciblées en constante évolution utilisées par les criminels qui 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.

L'évaluation des vulnérabilités assume cette tâche pour vous : les appareils et logiciels sur le réseau sont analysés à la recherche des points faibles susceptibles d'être exploités. Une fois ces lacunes localisées, la gestion des correctifs est en mesure de les combler en installant les mises à jour requises ou en réparant toutes les machines sur votre réseau.

Lorsqu'elle est mise en œuvre parallèlement à une stratégie efficace de gestion des correctifs, l'évaluation des vulnérabilités peut vous aider à conserver une longueur d'avance sur les cyber-criminels. Marche à suivre :

- **Restez à jour** : les logiciels obsolètes, sur des serveurs comme sur des postes de travail, exposent les entreprises à des attaques. Les analyses logicielles automatisées permettent une détection et une hiérarchisation rapides des vulnérabilités.

Kaspersky Systems Management assure le déploiement automatique de correctifs et de mises à jour dans des délais très courts pour les logiciels Microsoft et autres. Pour plus de contrôle, les administrateurs sont informés du statut d'installation des correctifs. L'exécution des correctifs non essentiels peut être repoussée après les heures de bureau et pourra se faire même si les ordinateurs sont éteints grâce à la fonction de réveil à distance Wake-on-LAN. La diffusion Multicast permet une distribution locale des correctifs et mises à jour sur les sites distants, réduisant ainsi les besoins en bande passante.

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.

- **Émettez des rapports** : lancez des rapports sur les analyses et obtenez une connaissance plus fine de la sécurité informatique de votre entreprise. Étudiez et signalez les points faibles potentiels, suivez les changements et obtenez une vision détaillée du statut des correctifs de chaque appareil et de chaque système sur le réseau.

Les attaques ciblées, les menaces persistantes sophistiquées, les attaques automatisées et les vulnérabilités « zero-day » réduisent considérablement le délai entre la détection des vulnérabilités et l'exploitation des failles. En automatisant et en planifiant l'évaluation régulière et la mise en œuvre des correctifs, les administrateurs informatiques peuvent rationaliser ces processus sans nuire à l'efficacité.

6. GESTION CENTRALISÉE ET CONTRÔLE DES ACCÈS BASÉ SUR LES RÔLES (RBAC)

La centralisation et l'automatisation des principales tâches de sécurité, de configuration et de gestion, telles que l'évaluation des vulnérabilités, la distribution des correctifs et mises à jour, la gestion des inventaires et le déploiement d'applications, permettent de gagner du temps mais aussi de gagner en sécurité.

Une seule console d'administration intégrée, Kaspersky Security Center, permet de gérer la sécurité des systèmes pour les postes de travail, les appareils mobiles et les terminaux virtuels sur l'ensemble du réseau à travers une seule interface. Dans les réseaux d'entreprise complexes, le contrôle des accès basé sur les rôles (RBAC) permet la personnalisation des vues de la console et des fonctionnalités en fonction des attributions, droits et privilèges de l'administrateur. Par exemple, un administrateur spécifique pourra consulter tous les domaines de gestion de la sécurité informatique sur la console, mais ne pourra modifier que les fonctions de gestion des vulnérabilités et des correctifs.

7. INTÉGRATION SIEM POUR LES ENVIRONNEMENTS D'ENTREPRISE

De nombreuses organisations, notamment les grandes entreprises, utilisent des systèmes SIEM pour collecter des journaux et d'autres données liées à la sécurité à des fins d'analyse. Les systèmes de sécurité capables de transmettre des rapports aux principaux systèmes SIEM contribuent à réduire la charge de travail de l'administrateur et les outils requis tout en simplifiant le processus de reporting de l'entreprise.

Kaspersky Systems Management s'intègre à IBM QRadar et HP ArcSight pour le transfert d'événements.

POUR FINIR

Les vulnérabilités logicielles sont aujourd'hui le point de mire des attaques ciblées et bien planifiées qui visent les entreprises de toutes tailles. La gestion efficace des applications et des correctifs, associée à l'évaluation des vulnérabilités et d'autres fonctionnalités de gestion des systèmes, peut offrir une approche intégrée de la sécurité informatique des entreprises.

Kaspersky Systems Management est un composant géré depuis la console Kaspersky Security Center, à l'aide de commandes et d'interfaces homogènes et intuitives, la finalité étant d'automatiser les tâches informatiques courantes et d'améliorer la sécurité de l'entreprise.


Twitter.com/
KasperskyFrance


Facebook.com/
KasperskyLabFrance


Youtube.com/
KasperskyFrance

Kaspersky Lab
www.kaspersky.fr

Tout savoir sur la sécurité
sur Internet :
www.securelist.com
http://www.viruslist.com/fr/

Rechercher un partenaire près de chez vous :
http://www.kaspersky.fr/partners/buyoffline/liste-des-partenaires

KASPERSKY lab