

Correctifs pour le centre de données

Les gros titres quotidiens qui parlent de vulnérabilités et autres menaces (sans parler des menaces inconnues et du risque d'en être victime) mettent les entreprises sous tension. Vous faites de votre mieux pour tenir à jour et sécuriser les logiciels système de vos utilisateurs. Mais qu'en est-il des serveurs de vos centres de données ? Dans le monde actuel, où les pirates peuvent accéder à des codes d'attaque pré-définis, les entreprises ont besoin d'une méthode efficace pour protéger les serveurs de leur centre de données sans épuiser leurs ressources IT.

Vos pratiques et mesures de sécurité doivent intégrer la gestion des correctifs afin de fortifier les serveurs, assurer la sécurité et la disponibilité des données et conserver la réputation de votre entreprise intacte. Vous devez déployer les correctifs de sécurité les plus récents, tout en continuant à consacrer du temps aux objectifs principaux de l'entreprise.

Vous avez besoin de contrôler précisément l'ensemble du processus d'application des correctifs (découverte et inventaire des correctifs, déploiement de tous les correctifs disponibles dans votre environnement) et de générer des rapports relatifs à ce processus, selon un calendrier qui convient à votre entreprise.

Mais de nombreuses entreprises ont du mal à tenir à jour leurs logiciels serveurs en appliquant les dernières mises à jour logicielles des systèmes d'exploitation et des applications tierces, notamment sur les systèmes Microsoft Windows® et les hyperviseurs VMware vSphere®. En effet, les centres de données présentent davantage de problèmes de gestion des correctifs que les systèmes clients, mais aussi des problèmes différents.

Détection et correction pour l'ensemble du centre de données

Pour assurer un degré élevé de précision des correctifs dans votre environnement, vous devez être à même d'effectuer facilement des scans de vos systèmes pour trouver les correctifs manquants, et de déployer les correctifs en respectant les stratégies dans l'ensemble de votre environnement. Sans une vision claire de votre environnement et sans informations détaillées sur les systèmes les plus vulnérables, il est impossible de comprendre les risques qui menacent votre entreprise. Mais la tâche n'est pas facile, en

raison de la multitude de configurations disponibles dans les centres de données modernes.

Les problèmes de temps et de budget associés aux environnements de centre de données virtuel (attendre l'amorçage des machines virtuelles (VM), application des correctifs, puis arrêt des machines) conduisent certaines entreprises à ignorer les environnements virtuels et à prendre des risques inutiles. Si l'on se soucie uniquement des serveurs physiques, l'entreprise est vulnérable et risque d'échouer aux audits. Vous devez être à même de trouver les vulnérabilités, de rechercher les correctifs manquants, et de déployer facilement ces correctifs sur les serveurs physiques et systèmes virtuels, sans perturber le travail des serveurs ou les activités de l'entreprise ; et lorsqu'il s'agit de conformité, impossible d'ignorer les systèmes hors ligne. Vous devez garantir la conformité des correctifs et fournir les mises à jour logicielles, que le système concerné soit sur le réseau ou déconnecté.

Réduction des délais d'application des correctifs

Sachant tout cela, combien de temps faut-il actuellement pour exécuter vos processus de mises à jour logicielles du centre de données ? Des mois, des semaines ? Pour limiter votre exposition, il faut réduire cela à quelques jours ou quelques heures.

Historiquement, 50 % des attaques se produisent dans les deux à quatre semaines qui suivent la publication des vulnérabilités. Un délai (SLA) imposé de 14 jours pour l'application des correctifs vous protégera de la majorité des exploitations. Mais les processus manuels, les pratiques et les multiples outils qui ne peuvent prendre en charge l'intégralité de votre environnement rendent votre gestion encore plus complexe, tout comme le temps nécessaire pour découvrir, définir et fournir des packages de mises à jour logicielles et appliquer ces correctifs critiques.

Que vos systèmes soient en ligne ou hors ligne, vous devez gagner du temps et consacrer vos rares ressources à des actions dont les résultats sont immédiats et à forte valeur ajoutée.

Il existe de nombreuses méthodes pour gagner du temps et limiter les risques. Par exemple, les modèles de correctif

permettent de gagner du temps et réduisent les risques chaque fois que vous mettez en place un nouveau serveur. La capacité à trouver rapidement toutes les VM hors ligne, et à appliquer des correctifs aux VM et aux modèles hors ligne peut vous faire gagner jusqu'à une heure par système. En vous assurant que les images hors ligne sont en permanence dans un état prêt au déploiement, vous êtes certain de pouvoir déployer une machine virtuelle sans vous demander si elle est vraiment à jour.

Pour gagner du temps, la méthode la plus efficace consiste à automatiser toutes les étapes du processus d'application de correctifs aux serveurs. Réfléchissez à la façon dont vous gérez actuellement l'évaluation des vulnérabilités effectuée par les fournisseurs. En repérant tous les correctifs liés aux CVE (Common Vulnerabilities and Exposures) et en créant automatiquement des groupes de correctifs pour la mise à jour, vous gagnez énormément de temps.

Enfin, vous avez besoin de simplifier la mise en conformité, en faisant le tri dans la masse d'informations concernant votre environnement et en accédant aux données à la demande. En confiant les données appropriées aux cadres, directeurs et propriétaires d'applications, la solution assure facilement la visibilité nécessaire pour réussir les audits, ainsi que des informations très à jour concernant votre position en matière de sécurité, pour une prise de décision efficace.

Liste de contrôle pour la gestion des correctifs

L'automatisation du processus de gestion des correctifs (de la découverte à l'évaluation, puis au déploiement) sur l'ensemble des postes de travail, et sur les serveurs physiques et virtuels en ligne et hors ligne, accélère la distribution des correctifs de sécurité critiques. Pour choisir la bonne solution de gestion des correctifs, vous trouverez dans le tableau ci-dessous les éléments à rechercher.

Ivanti peut vous aider

Avec ses outils robustes et simples d'application de correctifs aux serveurs qui répondent à tous vos besoins, Ivanti vous aide à protéger votre centre de données afin de gagner du temps et de l'argent, et de rester concentré sur les projets principaux de l'entreprise. Les outils Ivanti sont installés et opérationnels en quelques minutes et ils vous aident à découvrir, évaluer et corriger les systèmes de tout votre centre de données, automatiquement selon les stratégies que vous définissez. Nos outils simplifient l'application de correctifs à tous vos systèmes physiques et virtuels. Trouvez les postes de travail et serveurs en ligne et hors ligne, recherchez les correctifs manquants et déployez-les. Appliquez ensuite les correctifs à tous les éléments de votre installation, des OS aux applications en passant par les machines virtuelles, les modèles virtuels et même l'hyperviseur ESXi, grâce à l'intégration étroite de nos produits dans VMware.

Fonction	Description
Administration	Gestion fondée sur les rôles
Fonctions automatisées de découverte, d'inventaire et d'application des correctifs	Protection des postes de travail clients, des serveurs physiques, des serveurs virtuels, des hyperviseurs et des modèles
Mises à jour d'OS	Systèmes d'exploitation Windows et Linux
Correctifs d'application	Applications tierces et personnalisées
Automatisation de la liste « CVE à correctifs »	Importation de la liste d'évaluation des vulnérabilités de n'importe quel fournisseur
Contenu de correctifs	Accès à un catalogue de correctifs très complet
Déploiement de correctifs	Fonctionnement sans agent, avec agent et agent dans le Cloud
Prise en charge de l'annulation (rollback)	Possibilité de capture d'instantanés avant correctif
Activateur (Enabler) d'automatisation	API d'automatisation et d'orchestration
Collaboration	Partage d'état et vérification de la conformité des correctifs avec d'autres utilisateurs
Rapports	Tableaux de bord en temps réel et rapports personnalisables

Copyright © 2019, Ivanti. Tous droits réservés. IVI-2336 11/19 BB/MK/DL

En savoir plus



www.ivanti.fr



+33 (0)1 49 03 77 80



contact@ivanti.fr