Processus de gestion des correctifs

Depuis toujours, la gestion des correctifs est une tâche dont personne ne veut. Les administrateurs n'ont pas la visibilité complète ni les ressources nécessaires pour corriger les vulnérabilités toujours plus critiques, les risques liés aux changements font craindre le pire aux décideurs et les utilisateurs n'ont pas conscience de la criticité de ces mises à jour.

En tant que leader mondial de la gestion des correctifs, Ivanti se doit de vous proposer une organisation permettant de simplifier le travail des administrateurs, de gérer au mieux les risques liés aux changements et faciliter les interactions avec les utilisateurs.

Ce document décrit un exemple de processus à suivre afin de s'assurer que le déploiement des correctifs systèmes ou applicatifs puisse se dérouler dans les meilleures conditions.

Automatiser les analyses de vulnérabilités

A chaque vulnérabilité son patch ! Cet adage plutôt simpliste reflète bien la capacité des éditeurs à produire des correctifs après l'identification d'une vulnérabilité dans leurs produits.

Ainsi, à chaque publication d'un nouveau correctif, de nouvelles vulnérabilités sont rendues publiques et peuvent ainsi être ciblées par des codes malveillants.

Avant de mettre en marche le déploiement global du correctif associé, il faut commencer par connaître l'étendue du risque lié à ces nouvelles vulnérabilités.

Les scans de vulnérabilités et les rapports associés fournis dans les produits Ivanti vous permettront de connaître en permanence l'état de risque.

L'ensemble des définitions fournies par nos laboratoires seront déployées sur votre parc pour vérifier la présence ou non d'une vulnérabilité système ou applicative. Ainsi, quel que soit le produit utilisé, vous aurez toujours une vue globale des vulnérabilités présentes sur vos systèmes ainsi qu'une visibilité sur le travail de remédiation à effectuer.

Maîtriser les risques

Les outils d'analyse des vulnérabilités d'Ivanti permettent de connaître précisément l'état du risque sur l'ensemble des systèmes.

En étudiant la liste des vulnérabilités, vous pourrez déterminer avec précision quels sont les systèmes les plus à risques et concentrer vos efforts sur les opérations de remédiations les plus efficaces.

Automatiser les tâches les moins risquées

Comme pour votre antivirus, les définitions des vulnérabilités et des correctifs associés peuvent être téléchargées automatiquement.

Les packages des correctifs les plus critiques pourront également être téléchargés depuis Internet pour simplifier la gestion du déploiement.

L'application des définitions et les scans associés sont sans risque pour la plupart des systèmes, ainsi la plupart de nos clients automatisent les scans de vulnérabilités afin de déterminer le plus rapidement possible les actions à mener.

Définir un périmètre pilote

Le changement lié au déploiement d'un correctif sur un parc de machines n'est jamais sans risque, aussi, la méthode de validation du correctif est importante.

Le changement doit être anticipé en validant le bon fonctionnement des correctifs sur un ensemble de machines non critiques représentatif du parc.

Si un environnement de qualification est disponible dans votre infrastructure, les correctifs doivent en premier lieu être déployés sur cet environnement. Leur déploiement peut même être automatisé sur cet environnement afin de valider que les définitions que nous avons fournies fonctionnent dans votre contexte applicatif.

Si cet environnement de qualification n'est pas disponible, un ensemble de machines doit être défini en tant que périmètre pilote. Le choix de ce périmètre pilote peut se faire de différentes manières afin d'être le plus représentatif du parc :

- On définit de manière aléatoire un ensemble de machines pilotes, ce tirage au sort peut être effectué 3 ou 4 fois par an afin de ne pas cibler toujours les mêmes machines.
- On définit un ensemble d'utilisateurs volontaires qui devront être informés du déploiement afin d'obtenir un retour rapide du bon fonctionnement du changement.
- On cible en priorité des machines non critiques

Dans tous les cas, les machines les plus critiques (contrôle de production, VIP, nomades fréquents, etc.) ne devront pas être incluses dans le périmètre pilote.

La sélection des correctifs à valider se fera en fonction de la criticité des vulnérabilités détectées ou en fonction des évolutions que la DSI souhaite mener.

Quelle que soit la plateforme utilisée, la solution Ivanti permettra de définir un processus de remédiation en appliquant des groupes de correctifs à un groupe de machines. Cette phase sera très importante pour la validation fonctionnelle du correctif avant de passer à un déploiement global.

Gérer le retour arrière

Si la plupart des correctifs systèmes peuvent être désinstallés, c'est loin d'être le cas pour les patchs applicatifs.

Aujourd'hui, la plupart des correctifs fournis par les éditeurs d'applications tierces sont souvent des installateurs complets prenant en charge la montée de version ou la désinstallation de la version précédente.

La plupart des correctifs applicatifs permettront à l'application de fonctionner sans changements majeurs mais il se peut que certains correctifs ne puissent pas s'intégrer correctement dans l'environnement de production.

Si l'éditeur a rendu possible le retour arrière, la solution Ivanti permettra de rétablir la situation d'origine mais dans la grande majorité des cas, l'application actuelle devra être désinstallée et l'ancienne version redéployée sur les postes constituant le périmètre pilote.

Le correctif problématique doit alors faire l'objet d'une campagne de remédiation spécifique impliquant souvent les équipes de développement de l'éditeur.

Déployer rapidement

Une fois le correctif validé, le déploiement doit être planifié dans les plus brefs délais.

La planification des déploiements doit être réalisée en accord avec les contraintes de production mais en prenant en compte le risque lié à l'absence du correctif alors que la vulnérabilité peut être exploitée à tout moment par un code malicieux.

Le déploiement des correctifs serveurs est souvent le moins problématique car ceux-ci sont toujours accessibles et disposent dans la plupart des cas de plages de maintenance propices aux coupures de services ou au redémarrage. Les installations des correctifs serveurs sont ainsi souvent planifiées le dimanche entre 2H et 5H alors que les mises à jour

des postes de travail sont souvent réalisées le mercredi après-midi.

Le déploiement des correctifs peut être traités de différentes manières en fonction du type de postes (fixes ou portable) et en fonction de leur rôle (bureautique ou production) :

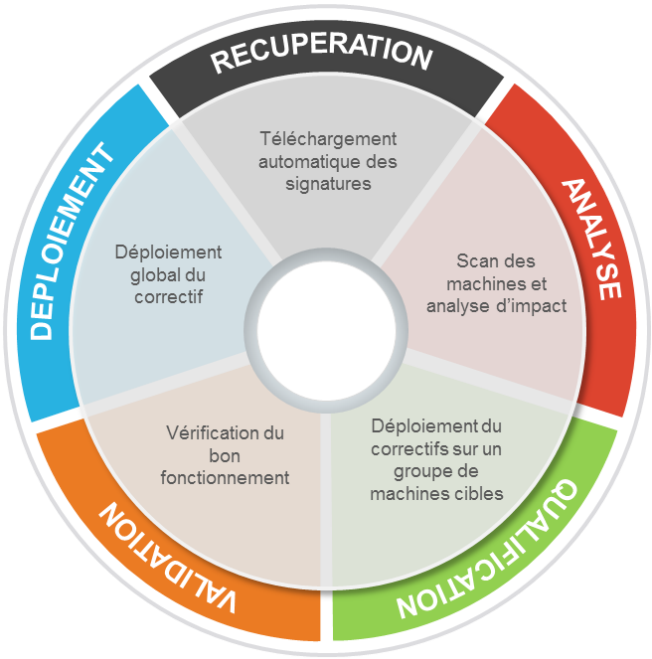
- L'interaction avec l'utilisateur est souvent la meilleure option, une fenêtre popup demande à l'utilisateur s'il souhaite installer les correctifs ou redémarrer sa machine. Une période de grâce de quelques jours peut être accordée avant de forcer l'installation du correctif.
- L'application du correctif sans interaction avec l'utilisateur est le meilleur moyen de s'assurer d'un déploiement rapide. Les correctifs nécessitant les plus critiques ne seront appliqués qu'au redémarrage de la machine. L'expérience utilisateur lors de l'arrêt ou du redémarrage de la machine peut être altérée et le fonctionnement des applications également.
- Grâce aux fonctionnalités de PoE embarquées dans la plupart des postes fixes, ceux-ci peuvent être redémarrés en dehors des périodes de production afin d'appliquer les correctifs. A l'issue de l'installation, le poste sera redémarré afin de terminer les installations des correctifs et une tâche d'arrêt sera planifiée une fois le redémarrage effectué. Cette solution peut s'appliquer à tous les réseaux disposant en grande majorité de poste fixes. Les postes portables ou nomades seront traités par l'une des deux premières méthodes.

Dans tous les cas, une communication globale devra être adressées aux différents services de gestion des utilisateurs (support, maintenance, responsables) afin de s'assurer que l'information concernant le changement sera bien diffusée. Les utilisateurs peuvent également être prévenus par une note de service mais ce scénario est souvent une option déconseillée.

Un processus continu

Le processus de détection et de remédiation des vulnérabilités doit être continu. En dehors des correctifs Microsoft qui sont livrés à date fixes, la plupart des éditeurs diffusent des correctifs dès qu'une faille est détectée et corrigée.

Le processus contient 5 étapes.



- Récupération des correctifs
- Scan et analyse d'impact
- Qualification sur le périmètre pilote
- Validation du bon fonctionnement
- Déploiement global

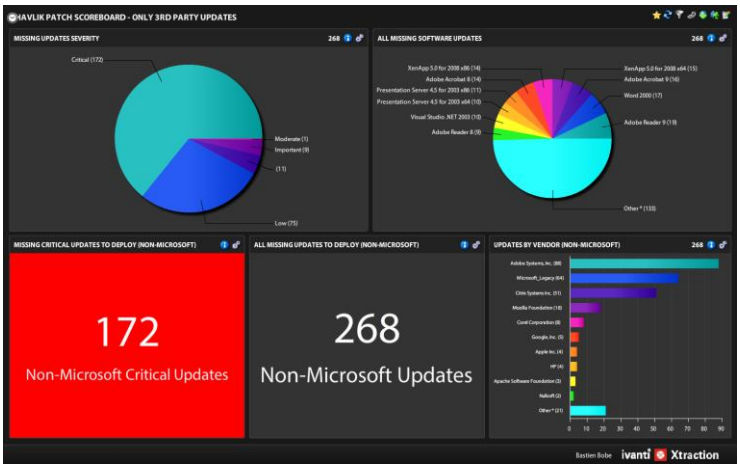
Après chaque déploiement, les administrateurs devront contrôler le bon déroulement de l'opération afin de limiter les risques et gérer le changement sereinement.

Les solutions Ivanti permettent d'automatiser la plupart des tâches décrites dans ce processus en simplifiant la gestion des scans de vulnérabilités, en automatisant le téléchargement des correctifs et en s'assurant du déploiement rapide et efficace des correctifs.

Sécurité renforcée

Les applications représentent désormais un plus grand risque pour votre sécurité que le système d'exploitation. Ivanti Patch réduit le risque lié aux applications en appliquant des correctifs pour des centaines d'éditeurs, notamment Adobe (Reader), Apple (iTunes), Oracle (Java), Google (Chrome), Firefox et bien d'autres. Mettez à jour même les applications les plus complexes.

Ivanti compte de nombreuses années d'expérience de l'application de correctifs dans l'entreprise. Il vous apporte ainsi les données de correctifs prétestés les plus précises et vous permet d'appliquer instantanément des correctifs aux applications tierces.



Les correctifs s'exécutent en mode silencieux et vous fournissent la version de la mise à jour logicielle appropriée pour votre entreprise et évitent l'installation par barre d'outils.

Retour sur investissements

"*Avec Ivanti Patch nous économisons 25K€ par mois ! Nous avons plus de trente correctifs, hors Microsoft, à déployer sur chaque poste. "* **N. Pell, IT Security Manager chez Nestlé.** *"Il nous fallait une journée entière pour déployer un seul patch. C'est en effet très long de récupérer les mises à jour, de les charger dans l'outil, de valider le fonctionnement du package, de le qualifier sur un environnement de pré-prod puis sur celui de production. Avec trente correctifs ce n'était plus envisageable et par ailleurs nous n'étions plus protégés. Le calcul est simple, une journée d'un de nos administrateurs IT pour chaque correctif, multiplié par 30 correctifs à déployer. Après intégration dans SCCM et 6 mois d'utilisation, nous avons configuré Ivanti Patch pour une mise à jour des correctifs tous les 15 jours. C'est pour nous l'idéal afin d'assurer la sécurité optimale."*

"*Ivanti Patch est une solution opérationnelle. Elle fonctionne de manière très visuelle grâce à des tableaux de bord simples afin d'identifier les failles de sécurité. Notre projet « Ivanti Patch » a été mené en un temps record, avec d'excellents résultats. Les correctifs nous assurent une très bonne gestion des vulnérabilités. Chez Lisi Automotive, nous sommes devenus patching addict !* " **Didier Parent, DSI chez Lisi Automotive.**