

AUTOMATISATION DES MISES À JOUR DE SÉCURITÉ

RÉDUISEZ VOTRE FENÊTRE DE VULNÉRABILITÉ ET FAVORISEZ LA RÉTENTION DE VOTRE ÉQUIPE TI

Avec de nouvelles vulnérabilités découvertes à toutes les semaines, **il est devenu impossible d'exécuter les mises à jour de sécurité manuellement sans accuser un sérieux retard**. Une charge de travail considérable, souvent exécutée de soir et de fin de semaine, qui épuise votre responsable TI tout en maintenant votre entreprise à risque d'attaques parce qu'insuffisante. **Dans un contexte de pénurie de main-d'œuvre où la rétention des ressources est un enjeu, on est à l'ère d'automatiser, comme en usine.**

La plupart des attaques sont causées par la négligence des mises à jour. Ces dernières deviennent alors des portes d'entrée pour les cybercriminels. Le délai entre la découverte d'une vulnérabilité et l'apparition d'un virus ou d'un ver se mesure désormais en jours ou en semaines plutôt qu'en mois. Bref, il faut faire vite!

La gestion des correctifs est souvent considérée comme une tâche banale. Cliquez simplement sur « mettre à jour » et c'est tout. Mais en réalité, il y a beaucoup plus que cela.

2B.UPDATED EST UN SERVICE GÉRÉ QUI INCLUT :



- La gestion automatisée du processus de mises à jour.
- Le matériel et les licences.
- Le support et la mise à niveau de la solution.
- L'analyse de rapports et la personnalisation.
- Des services-conseils pour améliorer votre niveau de sécurité.
- Des rencontres de gouvernance.

UN PROCESSUS EN 6 ÉTAPES :

Le but des mises à jour est de corriger les problèmes, de régler les vulnérabilités et d'améliorer les fonctionnalités du produit qui sont essentielles à la stabilité et à la performance d'une infrastructure TI.

Les mises à jour se doivent d'être évaluées, testées et appliquées. **L'automatisation facilite désormais le suivi des meilleures pratiques et permet à l'entreprise de protéger ses systèmes critiques des vulnérabilités connues.** La première étape consiste à mettre en place une politique dans le but d'être proactif au lieu d'être réactif.

Le processus devrait reposer sur l'automatisation, en **6 étapes** :

- 1 Accessibilité à votre **inventaire à jour** pour être au fait de l'ensemble des équipements qui sont connectés sur votre réseau;
- 2 **Détection, en temps réel**, des logiciels non protégés qui mettent votre entreprise à risque;
- 3 **Notification**, soit l'avis d'une vulnérabilité et d'une mise à jour disponible pour y remédier;
- 4 Tests en laboratoire pour vérifier **la compatibilité avant déploiement** afin d'éviter les pannes de systèmes lors des mises à jour;
- 5 **Déploiement progressif** des correctifs;
- 6 **Extraction de rapports**, confirmant que l'ensemble des composants de votre réseau a bien été sécurisé.

La sécurité de votre réseau nécessite une vigilance constante. Dans un contexte de pénurie de main-d'oeuvre et de multiplication des mises à jour due aux failles de sécurité, l'automatisation devient primordiale. Le temps de votre administrateur de réseau peut ainsi être utilisé à des projets à valeur ajoutée pour votre organisation, qui stimuleront son intérêt et **favoriseront une meilleure rétention.**

AUTOMATISATION DES MISES À JOUR DE SÉCURITÉ

AVANTAGES

- 1 **Amélioration du processus de sécurité face aux cyberattaques.**
- 2 **Identification en temps réel des périphériques non protégés.**
- 3 **Réduction des risques** de vulnérabilité par la rapidité de déploiement des mises à jour et la capacité de les effectuer au fur et à mesure.
- 4 **Sécurise** l'ensemble des composantes du réseau.
- 5 **Évite de négliger les mises à jour.**
- 6 **Évite les pannes de système** causées par les mises à jour grâce à une validation en laboratoire au préalable.
- 7 **Extraction de rapports** confirmant que l'ensemble des équipements a été mis à jour.
- 8 **L'entreprise bénéficie des nouvelles fonctionnalités** amenées par les mises à jour ainsi que d'une stabilité supérieure.
- 9 **Optimisation du processus de prise d'inventaire :**
 - Vue 360 sur les équipements et logiciels connectés sur le réseau.
 - Inventaire complet mis à jour.
- 10 **Optimisation de la gestion de l'inventaire :**
 - Accessibilité, en tant qu'administrateur, à l'inventaire de l'entreprise.
 - Accès rapide à l'information sous forme de rapports.
- 11 **Diminution des appels de support** causés par des versions de logiciels différentes.
- 12 **Meilleure expérience client** en permettant un suivi en temps réel avec l'utilisateur lors d'interventions et optimisation du temps de gestion lors des mises à jour.