Gestion des mises à jour et sécurité

Risques cyber liés à la mauvaise gestion des mises à jour

La gestion des mises à jour est un élément essentiel de la sécurité des systèmes et des données. En effet, négliger les mises à jour **expose les entreprises à des vulnérabilités exploitables** par des attaquants. Ainsi, ils pourraient accéder aux données sensibles, voire perturber la continuité des activités de l'entreprise. **La gestion proactive** des mises à jour **est donc impérative** pour garantir la protection des SI.

Types de mises à jour logiciels

- **Les mises à jour correctives:** ce sont des mises à jour publiées pour corriger les vulnérabilités de sécurité découvertes dans les logiciels, les bugs de fonctionnement ou de compatibilité.
- **Les mises à jour de version :** Ce sont des mises à jour qui apportent des améliorations fonctionnelles, des nouvelles fonctionnalités et des optimisations de performance.

Avantages des mises à jour

- **Amélioration de la sécurité :** Les mises à jour permettent de corriger les vulnérabilités découvertes dans les versions précédentes, réduisant ainsi le risque de leurs exploitations et de violation des données sensibles.
- **Optimisation des performances :** Les mises à jour incluent souvent des corrections de bugs et des améliorations de performance, ce qui contribue à rendre le logiciel plus stable et participe à l'amélioration de sa disponibilité.
- **Garantie de conformité :** Les mises à jour contribuent à assurer la conformité réglementaire, notamment pour la protection des données sensibles. Elles peuvent comporter des ajustements conformes aux évolutions des normes ce qui permet de prévenir les sanctions liées à la non-conformité réglementaire.

Bonnes pratiques dans le cadre de la gestion des mises à jour

- **L'Identification de l'ensemble des actifs :** dresser une liste exhaustive de tous les équipements (ordinateurs, routeurs, etc.) et logiciels (systèmes d'exploitation, applications, etc.) en vue de mettre en œuvre les mises à jour requises.
- **La veille proactive :** Maintenir une veille proactive sur les mises à jour de sécurité publiées par les fournisseurs de logiciels et les organismes de sécurité pour être informé des dernières vulnérabilités et correctifs disponibles.
- **Le téléchargement des mises à jour à partir des sites officiels :** Pour éviter les risques d'installer des logiciels malveillants ou de faux correctifs, il est crucial de télécharger les mises à jour uniquement à partir de sites officiels des éditeurs de logiciels.
- **L'application immédiate des mises à jour :** Les mises à jour contiennent souvent des correctifs critiques pour combler les vulnérabilités potentielles, il est donc recommandé de les installer immédiatement.
- **L'automatisation de l'installation des mises à jour :** Des outils pour l'automatisation de la gestion des mises à jour sont disponibles, leur utilisation permet de simplifier le processus et de s'assurer que les systèmes sont constamment à jour.

Ressources liées à la gestion des mises à jour

- Le **Guide d'Hygiène** de **ANSSI** concernant la sécurisation d'un SI incluant un chapitre sur la gestion des mises à jour **[PDF]**
- Les alertes du **CERT-FR** autour des **mises à jour** et des **correctifs critiques** **[Site WEB]**
- Les alertes du **CERT santé** autour des **mises à jour** et des **correctifs critiques** **[Site WEB]**
- Un article de la plateforme **CYBER MALVEILLANCE** sur les **bonnes pratiques** de gestion des mises à jour **[Site Web]**