La minute du PSIR

02 Mars 2022 - # 44

Pourquoi et comment gérer ses mises à jours ?

Les appareils numériques et les logiciels que nous utilisons au quotidien sont exposés à des failles de sécurité. Ces failles peuvent être utilisées par des cybercriminels pour prendre le contrôle d'un ordinateur, d'un équipement mobile ou encore d'une montre connectée. Face à ces risques, les éditeurs et les fabricants proposent des mises à jour (patch en anglais) visant à corriger ces failles. Si l'opération de mise à jour est souvent ressentie comme une contrainte, il s'agit pourtant d'un acte essentiel pour se protéger. Voici quelques bonnes pratiques à adopter pour vos mises à jour.

NIVEAU DE DIFFICULTÉ

Services/outils

PERSONNES CONCERNÉES

1. Pensez à mettre à jour sans tarder l'ensemble de vos appareils et logiciels

Ordinateurs, téléphones, systèmes d'exploitation, logiciels de traitement de texte, objets connectés... nous utilisons un grand nombre d'appareils et de logiciels. Il suffit qu'un seul ne soit pas à jour et soit exposé à une faille de sécurité pour ouvrir une brèche dans votre environnement numérique. Afin d'empêcher les cybercriminels d'utiliser ces failles de sécurité pour vous pirater et vous dérober des informations personnelles sensibles, il est primordial de réaliser les mises à jour de vos équipements dès qu'elles sont disponibles.

Différents types de mises à jour

- **Les mises à jour importantes ou critiques** corrigent les failles de sécurité qui peuvent être utilisées pour pirater votre équipement
- **Les mises à jour de version** apportent en général de nouvelles fonctionnalités et corrigent également des failles de sécurité. Ce type de mise à jour peut être payant.

2. Téléchargez les mises à jour uniquement depuis les sites officiels

Seuls les sites ou dispositifs officiels des éditeurs et fabricants vous garantissent au mieux que les mises à jour que vous allez installer ne sont pas infectées par un virus. À l'installation de vos mises à jour, soyez attentif aux éventuelles conditions d'utilisation ou cases pré-cochées qui pourraient valoir acceptation de l'installation d'un autre logiciel non désiré (logiciels publicitaires, par exemple).

3. Activez l'option de téléchargement et d'installation automatique des mises à jour

Si le logiciel le permet, configurez-le pour que les mises à jour se téléchargent et s'installent automatiquement. Avec cette fonctionnalité, vous disposerez ainsi de la dernière version à jour de la solution de l'éditeur. Assurez-vous également que la mise à jour fonctionne par une vérification manuelle, au besoin.

4. Planifiez les mises à jour lors de périodes d'inactivité

Lorsqu'ils interrompent une activité personnelle ou professionnelle (visionnage d'une vidéo, rédaction d'un courriel…), les messages indiquant la disponibilité d'une mise à jour sont souvent ignorés car le processus de mise à jour peut être ressenti comme une contrainte. En effet, la mise à jour peut prendre du temps, allant de quelques secondes à plusieurs minutes ou heures, selon les cas. Aussi, profitez de périodes d'inactivité pour effectuer vos mises (déjeuner, réunion, de nuit…).

5. Méfiez-vous des fausses mises à jour sur internet

En naviguant sur Internet, il arrive que des messages prenant l'apparence d'alertes de mises à jour apparaissent à l'écran : fausses publicités sur des sites Internet ou fenêtres (pop-up en anglais) malveillantes. Restez extrêmement vigilant car il peut s'agir d'une technique pour vous inciter à installer une prétendue mise à jour qui serait en réalité un virus.