



CASES articles

La mise à jour des programmes protège des cyberattaques

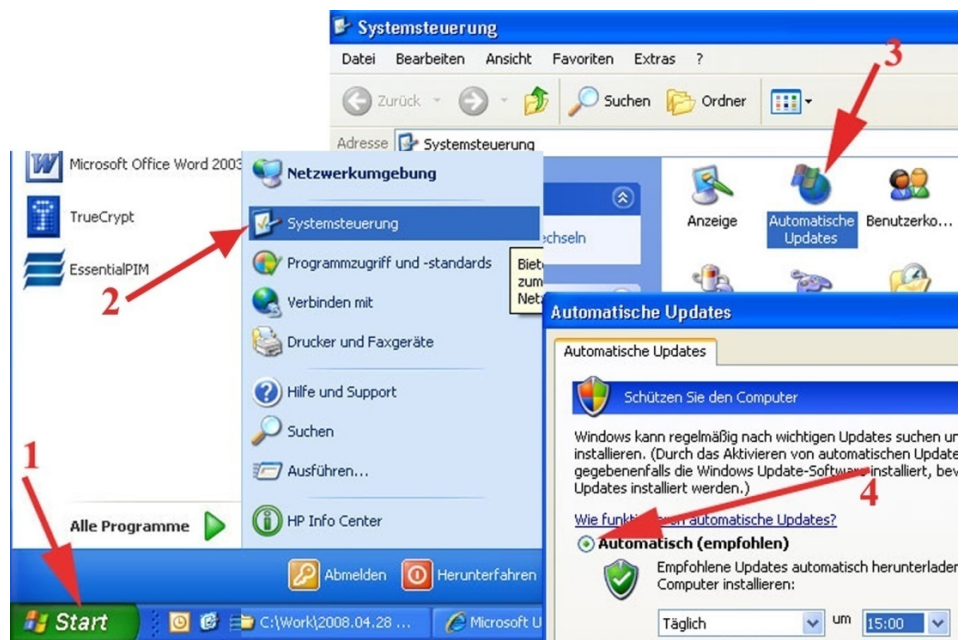
Les patches améliorent la sécurité informatique

Pour plus de sécurité, adoptez les réflexes CASES !

Une règle d'or - Les patches réduisent le risque de devenir victime des pirates informatiques

Les formes d'attaque employées par les pirates informatiques sont de plus en plus sophistiquées. Outre une bonne dose de méfiance, les usagers d'Internet doivent également disposer de moyens de protection techniques, installés sur leur ordinateur. Ils doivent également corriger les éventuelles failles de sécurité des programmes et systèmes d'exploitation installés sur leur machine. Dans ce cadre, Windows, Macintosh et Linux proposent aux utilisateurs une solution simple : la mise à jour automatique. Cette fonction permet d'appliquer efficacement et simplement une des règles d'or de la sécurité informatique : La mise à jour régulière des programmes.

Le nombre de fonctionnalités des systèmes d'exploitation et des applications ne cesse de croître. Les programmes sont de plus en plus complexes et les vulnérabilités, également appelées failles de sécurité, ne peuvent être exclues. Ces failles de sécurité sont exploitées par les cybercriminels en vue d'installer des malwares sur l'ordinateur d'un utilisateur. Afin de donner à l'utilisateur la possibilité de combler ces failles de sécurité, l'industrie logicielle met régulièrement à disposition des programmes de correction gratuits – les patches. Un logiciel présentant une faille peut être comparé à une série de véhicules touchés par un défaut de fabrication, le patch équivaut alors au rappel des véhicules pour réparation de ce défaut.



Si de nouvelles failles sont détectées dans les systèmes d'exploitation et les programmes, celles-ci sont annoncées publiquement. Des patches correspondants sont ensuite gratuitement mis à la disposition des usagers d'Internet pour téléchargement. Windows, Macintosh et des variantes de Linux, comme Ubuntu, intègrent des services spécifiques à cet effet. Ils procèdent à la mise à jour automatique des systèmes d'exploitation et programmes concernés. Chaque propriétaire d'ordinateur peut ainsi facilement remédier aux failles de sécurité. Outre le fait de corriger ces failles, un patch peut également ajouter des fonctionnalités à un programme. Les utilisateurs disposent ainsi toujours de la dernière version de l'application.

Mise à jour automatique - comment procéder

Pour les systèmes d'exploitation Windows XP, Windows Vista, Mac OS X et Ubuntu (une variante répandue de Linux), chaque utilisateur peut aisément vérifier si la fonction de mise à jour automatique est bien activée.

Windows Vista

Sous Windows Vista, cette fonction est automatiquement activée dès l'achat du nouvel ordinateur. Un clic sur [Démarrer] puis sur [Panneau de configuration] et [Windows Update] permet de le confirmer.

Windows XP

Les usagers qui utilisent le système d'exploitation Windows XP peuvent également vérifier en quelques clics si la fonction de mise à jour automatique est bien activée. Dans un premier temps, il faut accéder au panneau de configuration en cliquant sur [Démarrer] puis sur [Panneau de configuration]. Si l'affichage classique est sélectionné, l'utilisateur peut ensuite

directement cliquer sur [Mises à jour automatiques] et vérifier les réglages de cette fonctionnalité : l'option [Installation automatique (recommandé)] devrait être cochée. La mise à jour devrait de plus être réglée sur [Tous les jours]. Si ce n'est pas le cas, il est recommandé de modifier les réglages en conséquence. Si, à l'issue de la première étape [Démarrer] [Panneau de configuration], l'affichage des catégories est sélectionné, l'utilisateur doit cliquer sur [Centre de sécurité]. Un clic sur [Mises à jour automatiques] lui permettra ensuite de vérifier ses réglages.

MAC OS X

Les usagers utilisant le système d'exploitation MAC OS X d'Apple cliqueront sur [Préférences Système], puis sur [Mise à jour de logiciels] afin de vérifier les réglages de la mise à jour automatique.

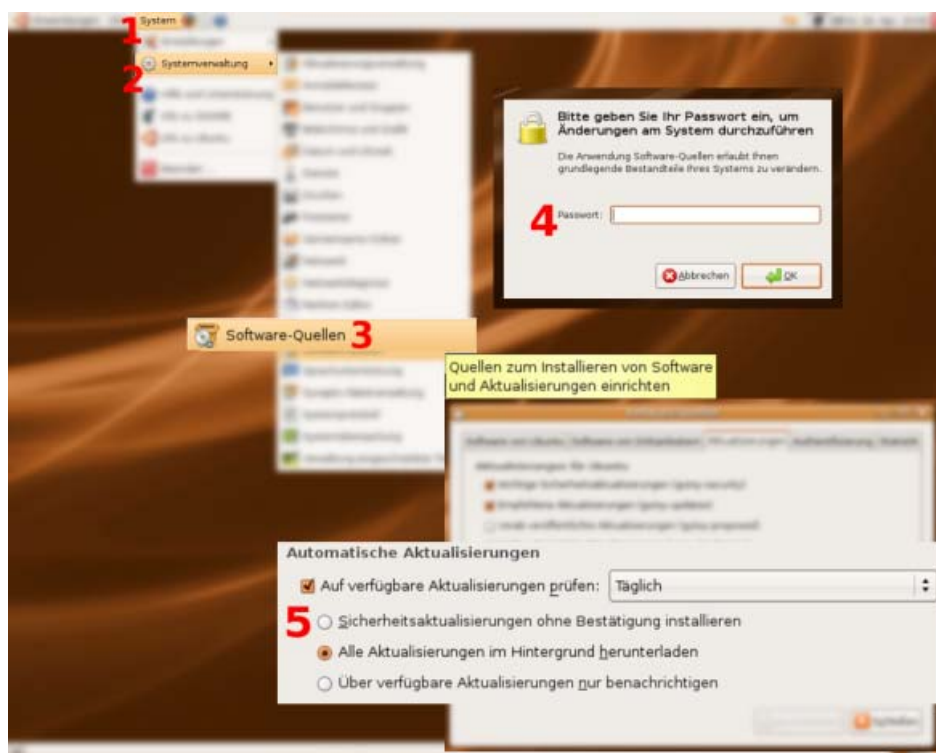
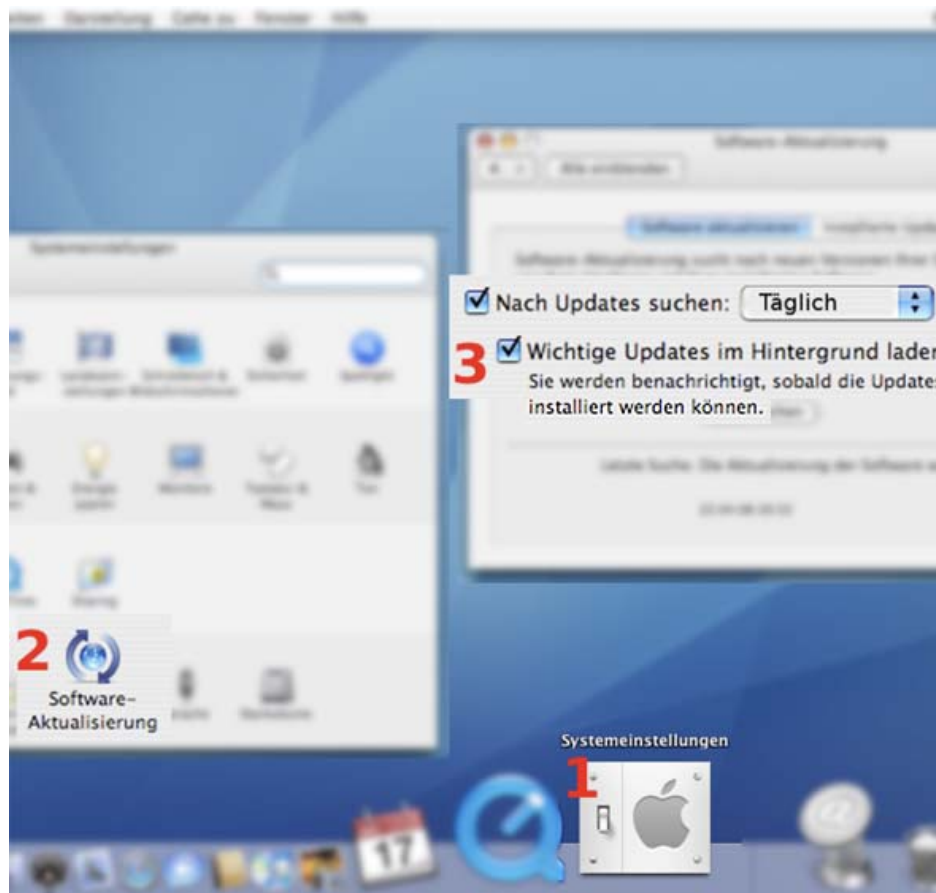
Variante de Linux Ubuntu

Afin de vérifier les réglages de leur système, les utilisateurs d'Ubuntu procéderont comme suit : [Paramètres du système] [Administration du système] puis [Sources de mises à jour]. Après saisie du mot de passe, l'utilisateur peut sélectionner [Mises à jour] et vérifier que [Recherche de mise à jour] est bien réglé sur [quotidiennement].

Mise à jour d'applications logicielles

Le cycle de vie d'un patch débute d'ordinaire par l'annonce publique de la détection de la faille de sécurité par le fabricant du logiciel ou par toute autre source. Cette annonce coïncide généralement avec la mise à disposition d'un patch correctif. La faille de sécurité peut ainsi être colmatée rapidement.

De nombreux utilisateurs installent sur leur ordinateur toutes sortes de logiciels qui ne disposent pas de fonctions de mise à jour automatique. Chacun d'eux devrait alors s'informer des failles de sécurité détectées et installer les patches correspondants. Le portail de sécurité de l'information du Luxembourg, www.cases.lu, informe les usagers d'Internet des failles de sécurité les plus importantes et des patches à mettre en œuvre.



« Un patch devrait porter une date, un numéro de version et des informations quant à la faille de sécurité concernée et aux systèmes et programmes qui sont touchés. En outre, des indications quant à l'installation du patch

ainsi que des informations de contact devraient être fournies », explique François Thill, responsable du portail luxembourgeois. Pour les entreprises, il est important de connaître les éventuelles conséquences liées à

l'installation d'un patch. Il leur est recommandé de tester les patches dans un environnement test avant de procéder à leur installation. L'installation d'un patch peut déclencher une réaction du pare-feu, celui-ci demandant à l'utilisateur de confirmer si l'exécution du programme doit être autorisée. Si le patch provient d'une source fiable, l'autorisation peut être confirmée.

Méfiance à l'encontre d'e-mails invitant à la mise à jour d'applications

Les cybercriminels ne tentent pas seulement d'exploiter les failles de sécurité et les mises à jour de programmes par le biais d'attaques directes – ils essaient également de le faire grâce à de fausses informations contenues dans des e-mails falsifiés. Des malwares camouflés en patches peuvent alors être joints à ces e-mails frauduleux. Les utilisateurs devraient traiter les courriers électroniques invitant à la mise à jour de programmes ou à la correction de failles de sécurité avec beaucoup de méfiance et de prudence. Il est recommandé de toujours se méfier de ce genre d'e-mail.

Dans le doute, l'utilisateur devrait consulter la page web du fabricant du logiciel et vérifier l'exactitude des informations. Les patches ne devraient être téléchargés que sur la page officielle du fabricant du logiciel ou provenir d'une autre source fiable.

Exemple concret : Accès à l'ordinateur grâce à des failles de sécurité touchant Adobe Flash Player.

De nombreux usagers d'Internet utilisent le logiciel Adobe Flash Player pour visionner des vidéos issues du web. Lors du concours de sécurité CanSecWest, organisé fin mars 2008, des experts de la sécurité de l'information ont découvert une faille de sécurité dans ce programme. Celle-ci permettait l'accès non autorisé à un ordinateur test équipé du système d'exploitation Windows Vista. Selon ces experts, l'accès à des machines équipées d'autres systèmes d'exploitation par le biais de cette faille dans Flash Player était également envisageable. Après communication de cette faille de sécurité à la société Adobe, celle-ci a procédé à la publication d'un patch correctif au profit des utilisateurs de Flash Player.

Conseils de sécurité :

Le portail de sécurité luxembourgeois www.cases.lu propose un récapitulatif illustré de la mise à jour automatique de programmes Microsoft, Macintosh et Ubuntu. Le propriétaire d'un ordinateur peut toutefois facilement perdre la vue d'ensemble sur tous les programmes installés sur sa machine. De plus, il dispose en général de peu de temps pour se tenir informé des dernières failles de sécurité connues. Posséder la totalité des programmes dans leur version la plus actuelle est donc presque impossible. L'industrie propose des solutions gratuites à ce problème. Exemple : le programme gratuit Personal Software Inspector de la société de sécurité de l'information Secunia. Il permet de détecter et d'actualiser les versions obsolètes de logiciels. Il est disponible sur le site <https://psi.secunia.com> et gère plus de 4200 applications.

Retrouvez les dossiers, fiches thématiques alertes et actualités sur:

www.cases.lu