



CASES articles

Connaissances et savoir-faire autour de l'Internet – petit récapitulatif

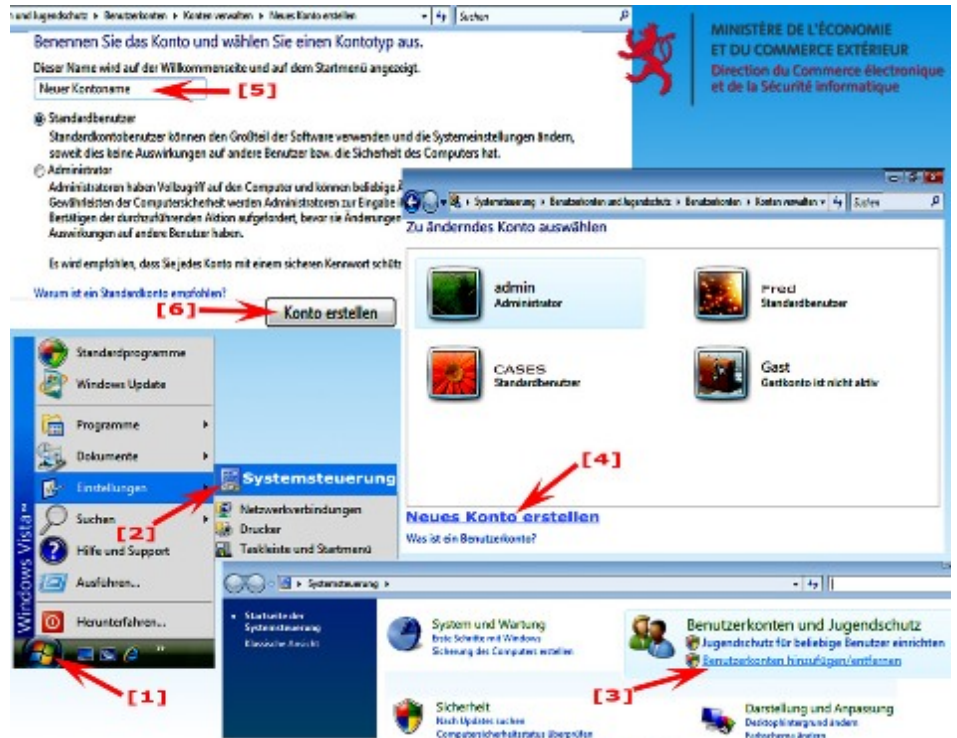
La vérification de sécurité de l'ordinateur

Pour plus de sécurité, adoptez les réflexes CASES !

Vérification des règles d'or de la sécurité sur un ordinateur

Parmi les cadeaux de Noël 2008 les plus populaires figurent, entre autres, les ordinateurs. Pour pouvoir profiter sans restriction d'un tel cadeau, il est conseillé d'effectuer une vérification de sécurité sur l'ordinateur. Cette vérification ne prend que quelques minutes et ne requiert aucune connaissance particulière. Tout un chacun – parents, grands-parents, homme ou femme – peut vérifier que l'ordinateur respecte bien les règles d'or de la sécurité informatique. Si des failles de sécurité sont détectées, elles sont en général facilement réparables, sans occasionner de coûts.

Une enquête du réseau social spin.de a démontré qu'outre les consoles de jeu et les téléphones mobiles, les ordinateurs comptent parmi les cadeaux de Noël les plus populaires pour l'année 2008. Pour démarrer la nouvelle année en toute sécurité, il convient de vérifier que l'ordinateur respecte bien six importantes règles de sécurité. Le système d'exploitation est-il mis à jour automatiquement ? Des comptes d'utilisateur spécifiques ont-ils été créés pour chaque utilisateur ? L'ordinateur dispose-t-il des moyens de protection techniques indispensables, tels qu'un logiciel anti-virus régulièrement mis à jour et un pare-feu activé et correctement paramétré ? Un programme anti-spyware régulièrement mis à jour est-il présent sur l'ordinateur et des mots de passe sécurisés sont-ils utilisés ?



Titre intermédiaire : Mise à jour automatique du système d'exploitation

Les failles de sécurité d'un ordinateur peuvent être réduites grâce à la mise à jour permanente et automatique de son système d'exploitation. Le système d'exploitation comprend les logiciels nécessaires pour gérer les données et pour démarrer la machine. De nos jours, il s'agit souvent de Windows XP ou Vista. Le système d'exploitation administre les différents composants, tels que la mémoire et les unités d'entrée/de sortie, et gère l'exécution des programmes. Étant donné qu'il s'agit là d'un nombre très important de programmes adaptés les uns aux autres, l'apparition d'erreurs involontaires pouvant générer des risques de sécuri-

té est fréquente. Afin d'écartier ces risques, il est recommandé d'avoir recours à la mise à jour régulière et automatique du système d'exploitation, souvent également appelée « update automatique ». Sous Windows XP et Vista, l'utilisateur a la possibilité de configurer son système de manière à ce que la mise à jour soit régulière et automatique. Chaque utilisateur peut facilement vérifier que son ordinateur est bien paramétré pour effectuer des « updates automatiques ». Sous Vista, il suffit de procéder comme suit pour le vérifier : DÉMARRER -> PANNEAU DE CONFIGURATION -> SÉCURITÉ -> CENTRE DE SÉCURITÉ -> Mises à jour automatiques activé/désactivé. Sous XP, la procédure est la suivante : DÉMARRER -> PANNEAU DE

CONFIGURATION -> MISES À JOUR AUTOMATIQUES. Si cette fonction est activée, l'ordinateur vérifiera de façon autonome la disponibilité de nouvelles mises à jour proposées par le fabricant. Si une telle mise à jour est disponible, elle est automatiquement téléchargée et installée.

Titre intermédiaire : **Création de comptes d'utilisateur spécifiques pour chaque usager**

La mise en service d'un ordinateur est très simple de nos jours : il suffit de brancher les câbles de connexion et l'utilisation peut commencer. Les utilisateurs devraient toutefois savoir que les fabricants ne dotent le système d'exploitation préinstallé sur un ordinateur, tel que Windows Vista ou XP, que d'un seul compte utilisateur : celui de l'administrateur.

L'administrateur (admin) d'un ordinateur dispose de tous les droits dans le système d'exploitation. Cela signifie qu'il peut modifier la totalité des paramètres sur l'ordinateur en question. Il possède par exemple le droit d'installer des programmes et de les effacer, ou encore de créer des comptes d'utilisateur supplémentaires, de les désactiver ou de les doter de droits spécifiques. L'utilisateur inconscient disposant des droits d'administrateur peut rapidement commettre une erreur de manipulation. Il est ainsi possible d'effacer des données importantes, telles que des photos ou des documents appartenant à d'autres membres de la famille. Un clic malencontreux, un message de l'ordinateur ou une requête de paramétrage mal compris(e), et l'utilisateur modifie sans le vouloir les réglages du système. Les conséquences peuvent être considérables : des données peuvent ainsi être irrémédiablement perdues. La restauration du système est un processus long et fastidieux, pouvant entraîner des coûts.

Dans la majorité des cas, l'ordinateur est également utilisé pour surfer sur l'Internet. Si cela est effectué avec les droits d'administrateur et que l'ordinateur subit une attaque non dé-

tectée et couronnée de succès par des cybercriminels, ceux-ci obtiennent les mêmes droits et sont ainsi en mesure de prendre le contrôle de l'ensemble du système informatique.

Tout comme pour la mise à jour automatique du système d'exploitation, l'administrateur peut facilement et rapidement réduire ce genre de risque de sécurité. Il suffit pour cela de vérifier de quels droits disposent les différents membres de la famille. Une seule personne devrait posséder le droit d'utiliser le compte administrateur. Ce compte ne devrait en aucun cas être utilisé pour surfer sur l'Internet. Un compte utilisateur doté de droits limités a-t-il été créé pour chaque personne utilisant l'ordinateur ? Un compte d'utilisateur spécifique a-t-il été créé pour les seules opérations de banque en ligne ?

La création de comptes d'utilisateur est simple. Pour les systèmes d'exploitation Windows Vista et XP, la procédure est la suivante : sous DÉMARRER [1] -> PANNEAU DE CONFIGURATION [2] -> COMPTES D'UTILISATEURS [3], l'administrateur peut créer un nouveau compte disposant de droits limités pour chaque utilisateur de l'ordinateur [4], [5], [6]. L'Internet devrait être utilisé exclusivement avec ce genre de compte d'utilisateur. Les utilisateurs peu expérimentés devraient toujours être dotés de droits limités. Ceci permet de rendre la tâche d'éventuels attaquants plus ardue.

Titre intermédiaire : **Protection technique indispensable**

L'équipement de sécurité fondamental d'un système informatique doit comprendre un logiciel anti-virus. À cet effet, l'industrie met même à la disposition des utilisateurs privés des anti-virus gratuits. Ceux-ci peuvent être téléchargés sur Internet et installés. Ensuite, il est nécessaire de paramétrer correctement le programme.

Pour que l'anti-virus soit en mesure de détecter les malwares les plus récents, il doit être mis à jour régulièrement. À cet effet, ces programmes disposent,

tout comme les systèmes d'exploitation, d'une fonction de mise à jour automatique. Il est indispensable de vérifier que l'ordinateur est bien équipé d'un logiciel anti-virus et que la fonction de mise à jour automatique de celui-ci est activée.

De plus, au moins une fois par mois il est recommandé d'analyser l'ensemble du système à l'aide du programme anti-virus. Cette fonction peut être activée en quelques clics. Les anti-virus sont également en mesure de détecter des malwares dans les fichiers joints d'e-mails, lesquels constituent le principal moyen de propagation des programmes malveillants. Un seul logiciel anti-virus doit être activé sur l'ordinateur ; dans le cas contraire, des dysfonctionnements peuvent en effet survenir.

Un logiciel dénommé pare-feu est un autre outil essentiel de la sécurité informatique. Il s'agit d'un programme permettant de réduire les risques de transmission incontrôlée de données vers l'ordinateur ou à partir de celui-ci. Un pare-feu correctement paramétré procède au contrôle de toutes les données entrant et sortant de l'ordinateur. Cela permet d'interdire les accès de tiers à la machine.

Un pare-feu est intégré à Microsoft Vista et XP. Celui-ci peut être vérifié, activé et paramétré sous DÉMARRER -> PANNEAU DE CONFIGURATION -> CENTRE DE SÉCURITÉ. Bien que Windows Vista et XP disposent d'un pare-feu intégré, il est recommandé d'installer un logiciel pare-feu supplémentaire. Ici aussi, l'industrie propose aux utilisateurs privés des solutions gratuites et néanmoins de grande qualité. Il n'est pas recommandé d'utiliser deux pare-feu simultanément ; après l'installation du second logiciel, le pare-feu intégré de Windows devrait donc être désactivé.

Une autre vérification de sécurité vise à détecter la présence de logiciels d'espionnage sur l'ordinateur. Cette vérification est réalisée à l'aide d'un programme anti-spyware.

De nombreux logiciels d'espionnage, ou spywares, sont utilisés pour analyser le comportement des utilisateurs sur Internet. Les données ainsi recueil-

lies sont exploitées à des fins commerciales, par exemple pour afficher des publicités taillées sur mesure pour l'utilisateur. Les spywares peuvent également générer des failles de sécurité dans un système, rendant impossible la mise à jour des logiciels impliqués dans la sécurité. Les spywares se protègent de l'effacement en exécutant plusieurs processus simultanément. À la fin d'un processus, un nouveau est immédiatement lancé et l'administrateur du système est privé des droits requis pour effacer les spywares. Ceci permet d'ailleurs de mieux comprendre l'importance de créer des comptes d'utilisateur dotés de droits d'accès limités.

Les ordinateurs nouvellement achetés ne disposent pas automatiquement de logiciels anti-spyware. Il est donc nécessaire de les installer soi-même. Tout comme pour les anti-virus et les pare-feu, des solutions gratuites viennent compléter les produits anti-spyware payants proposés aux utilisateurs privés. Avant l'utilisation d'un ordinateur, il est par conséquent important de vérifier qu'un programme anti-spyware est bien installé et que celui-ci est mis à jour régulièrement. Il convient également de s'assurer que le système est régulièrement analysé pour détecter les éventuels spywares.

La dernière vérification essentielle de sécurité concerne l'utilisation de mots de passe sécurisés. Un mot de passe

sécurisé comporte au minimum 8 caractères regroupant des lettres majuscules et minuscules, des chiffres et des caractères spéciaux. Les prénoms des membres de la famille ou les dates d'anniversaire ne devraient jamais être utilisés en tant que mots de passe. Tout comme les brosses à dents, ils ne devraient jamais être partagés et être changés régulièrement.

Le portail de la sécurité de l'information CASES, www.cases.lu, propose des guides détaillés relatifs aux processus de vérification de la sécurité d'un ordinateur ainsi que des références à des programmes de protection mis gratuitement à disposition des utilisateurs privés par l'industrie.

Retrouvez les dossiers, fiches thématiques alertes et actualités sur:

www.cases.lu