

Dix conseils sur la sécurité de l'information pour PME



De nos jours, les technologies de l'information sont considérées comme des facteurs de succès importants pour les PME dans l'atteinte de leurs objectifs de productivité et de rentabilité. Cependant, seuls, ces outils sont susceptibles à des failles de sécurité. Il faut donc que les PME jumellent ces outils à des tactiques et des stratégies de sécurité afin de se protéger, ainsi que leurs clients, face aux menaces qui existent. Voici donc dix conseils-clé afin d'améliorer votre sécurité de l'information et arriver à ces fins:

1. Formez vos employés aux principes de base

Établissez des politiques de sécurité de base, visant à protéger l'information qui transige dans votre organisation et communiquez celles-ci à vos employés régulièrement. Dans ces politiques, assurez-vous de décrire les comportements acceptables face à la sécurité ainsi que les pénalités pour la violation des règles établies.

2. Protégez l'information, les ordinateurs, le réseau contre les virus, les logiciels espions et malveillants

Installez, utilisez et mettez à jours régulièrement un antivirus sur tous les postes de travail et serveurs de votre organisation. Ce type de logiciel est facilement accessible à travers divers vendeurs. Assurez-vous de configurer l'antivirus pour qu'il se mette à jour automatiquement à un moment de la journée où l'usage du réseau est bas (ex. pendant la nuit). Encore mieux, faites en sorte que le logiciel balaye le réseau immédiatement après sa mise à jour.

3. Protégez votre connexion internet avec un coupe-feu

Un coupe-feu est un équipement (ou un logiciel) qui empêche l'accès à votre réseau informatique des intrusions non-autorisées provenant d'internet. Placez votre coupe-feu entre votre réseau local et l'internet. Si vous avez des employés qui travaillent de la maison, assurez-vous qu'ils soient également protégés par un coupe-feu.

4. Mettez à jour votre système d'exploitation et applications

Tous les vendeurs de systèmes d'exploitation régulièrement rendent disponibles des correctifs (*patch*) pour leur produit afin de corriger ses lacunes de sécurité et améliorer sa fonctionnalité. Configurez votre système d'exploitation et vos applications pour qu'ils intègrent automatiquement ces correctifs.

5. Faites des copies de sauvegarde de vos données d'affaires importantes

Il est très important de faire ces copies de sauvegarde régulièrement et ce, pour tous les postes de travail de votre organisation. Il est recommandé d'exécuter cette tâche hebdomadairement.

6. Ayez un contrôle d'accès physique à votre réseau

Empêchez une personne non-autorisée d'accéder à un ordinateur et à votre réseau informatique. Les ordinateurs portables sont des cibles de prédilection pour les voleurs. Assurez-vous que ceux-ci soient entreposés en lieu sûr lorsque que non-utilisés.

7. Sécurisez votre réseau sans-fil

Si vous utilisez ce type de réseau, assurez-vous qu'il soit caché et sécurisé. Pour cacher un réseau sans-fil, configurez votre router pour que celui-ci ne divulgue pas le nom du réseau, connu sous le nom de SSID (*Service Set Identifier*). De plus, activez l'option de chiffrement qui fera en sorte que le réseau sera protégé par un mot de passe. Finalement, il est important de changer le mot de passe original (du fabricant) du routeur.

8. Exigez un compte utilisateur individuel pour chaque employé

Assurez-vous que ceux-ci soient protégés par un mot de passe robuste et ne donnez les privilèges administratifs qu'aux responsables TI de confiance.

9. Limitez les permissions et l'autorisation à faire des installations

Ne donnez jamais l'accès complet au réseau à une personne unique. Les employés devraient avoir accès seulement aux ordinateurs qui leur permettent de faire leur travail. De plus, ces derniers ne devraient pas pouvoir installer de nouveaux logiciels sans autorisation.

10. Changez vos mots de passe régulièrement

Il est fortement recommandé de changer de mot de passe tous les trois mois. Tous les employés devraient faire de même.

Pour plus de conseils et de renseignements sur comment sécuriser votre PME, consultez le www.gardienvirtuel.ca