

les affaires

dossiers technologies pour pme

Assurer la sécurité informatique pour protéger l'entreprise

Conseils. Contrer les menaces requiert discipline et vigilance.

par Claude Giguère > dossiers@transcontinental.ca

Aucune PME peut prétendre être à l'abri des menaces informatiques. La plupart des entreprises utilisent Internet et certaines ont même un site transactionnel. Elles doivent prendre au sérieux les menaces informatiques et savoir les déjouer efficacement.

Quand une PME n'a pas les moyens de confier à une firme externe la gestion de sa sécurité informatique, Jason Bilodeau, analyste en sécurité des systèmes à l'Institut de la sécurité informatique du Québec (ISIQ), et membre du CRIM propose la démarche suivante. « Sur le plan de l'exploitation, il faut catégoriser ses actifs, faire une analyse des risques et former sa propre équipe de sécurité. Sur le plan technique, le point le plus important est de faire de la sensibilisation au niveau organisationnel et humain. »

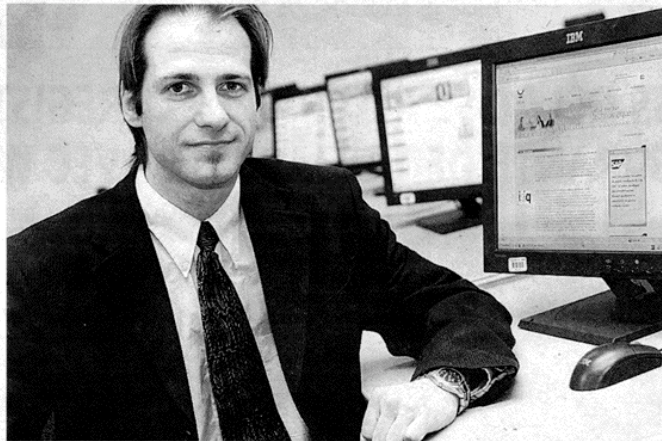
Une série de démarches

Parmi les mesures à prendre sur une base régulière pour assurer la sécurité, il y a :

- la fermeture des ports et services inutiles sur les serveurs et les postes de travail;
- la mise à jour régulière des logiciels et des abonnements à des services comme les anti-virus; et
- l'encryption des données et des communications.

Évidemment, un équipement informatique désuet n'est pas l'idéal, mais il faut prioritairement investir pour que les systèmes d'exploitation installés soient à jour. « Chaque système, chaque service peut devenir un point d'entrée; il est donc important de toujours être à jour. Un système d'exploitation doit impérativement être renouvelé si aucune mise à jour n'est disponible. Il en est de même pour les services », précise M. Bilodeau.

Par exemple, si quelqu'un se risquait à surfer sur Internet avec un ordinateur doté d'un système d'exploitation Windows 98, l'infection serait très probable, puisque Microsoft



Jason Bilodeau, de l'Institut de la sécurité informatique du Québec : « Sur le plan de l'exploitation, il faut catégoriser ses actifs, faire une analyse des risques et former sa propre équipe de sécurité. Sur le plan technique, le point le plus important est de faire de la sensibilisation au niveau organisationnel et humain. » [Photo : Yves Provencher]

ne fournit plus de mises à jour pour ce système désuet, encore utilisé dans plusieurs entreprises.

Cela dit, même avec un système récent tel Windows

XP, il est essentiel que toutes les mises à jour soient installées dès leur sortie. Choisir l'option de mise à jour automatique évite bien des soucis. Notons qu'un ordinateur fon-

ctionnant avec un système d'exploitation Windows non reconnu (copié ou piraté) ne pourra bénéficier de ces mises à jour et deviendra de plus en plus vulnérable à mesure

qu'apparaissent de nouvelles menaces.

Mêmes menaces, moins de ressources

Les PME, même bien intentionnées, ne sont pas à l'abri. « Il existe un faux sentiment de sécurité parmi les chefs de PME et nous entendons couramment dire : "Ça ne nous arrivera pas". Or, une entreprise de taille moyenne est exposée aux mêmes menaces pour la sécurité qu'une grande, bien qu'elle ne dispose généralement pas des mêmes ressources », dit Harry Bolner, vice-président de Fusepoint.

« Même si aujourd'hui la plupart des entreprises recourent à une quelconque technologie de protection des données, nombre d'entre elles sont dépassées par le nombre croissant d'attaques de virus, de pirates, de trafic non autorisé et d'autres intrusions. En outre, les employés mobiles qui téléchargent sans le vouloir des virus, des logiciels espions ou des publicités en étant à leur domicile ou à d'autres endroits suscitent une inquiétude grandis-

► **santé du point de vue de la sécurité** », ajoute M. Bolner.

Cet expert considère que les services informatiques de la plupart des PME n'ont pas le temps, les outils ou l'expertise nécessaires pour protéger leurs systèmes contre les menaces. « Les PME devraient connaître les risques qu'elles courent et se poser les questions difficiles, faire une analyse des répercussions éventuelles sur leur exploitation et se fier à des spécialistes pour s'assurer de ne pas faire partie des sombres statistiques. »

Patrick Naoum, vice-président, solutions clients, chez ESI Technologies, croit lui aussi que les risques sont trop souvent minimisés. Il note qu'un minimum d'attention doit être apporté à la sécurité, ne serait-ce que pour se conformer aux lois et règlements et aux bonnes pratiques, notamment en ce qui a trait à la protection des données personnelles.

« La majorité des PME ne sont même pas au courant des risques qui les menacent », dit M. Naoum, qui concède que selon l'utilisation qu'une entreprise fait des technologies de l'information, plus ou moins d'attention devrait portée à cette question.

Dans les autres cas, rien ne doit être laissé au hasard. « Il faut prioritairement établir un constat initial de l'état des choses en fonction de la valeur des actifs du client. Puis, établir le risque et la probabilité du risque sur ces actifs et systèmes. Et ensuite établir un plan de conformité et de remédiation. Cet exercice doit être fait au moins une fois par an, c'est comme une vérification financière et on devrait y accorder autant d'importance », dit M. Naoum.

Au quotidien, quelques conseils de base doivent être donnés aux employés, note Jason Bilodeau. « Il faut sensibiliser les gens, utiliser des pare-feu, des antivirus et anti-spyware, instaurer une politique de mots de passe difficile plus sûrs et éviter les mots de passe partagés, encrypter les données et les communications et garder les périphériques amovibles en lieu sûr et les chiffrer, le chiffrement n'étant cependant pas recommandé pour les sauvegardes. » †