E-accounting et security

Erwin Vercammen
Expert-comptable – Conseil fiscal

L'*e-accounting* concerne non seulement l'utilisation d'ordinateurs, de programmes et de l'électronique, mais fait également référence à l'inévitable sécurisation dont elle s'accompagne. Nos activités quotidiennes d'audit nous apprennent en effet que les problèmes ne résultent pas toujours de pratiques frauduleuses ou de corruption, mais peuvent également découler d'erreurs ou de maladresses innocentes. Ces problèmes peuvent nuire à la productivité. Il va donc sans dire que le moindre dysfonctionnement du système informatique risque de compromettre le fonctionnement de plus d'un bureau. À cet égard, nous avons jugé qu'il était opportun de faire toute la lumière sur la problématique de la sécurisation.

La sécurité se retrouve à plusieurs niveaux, que l'utilisateur doit reconnaître et respecter.

Il convient tout d'abord d'accorder une attention particulière à la *sécurisation de l'accès au niveau de la connexion*. Lorsque nous utilisons un environnement ASP, le fournisseur ASP se charge non seulement de la copie de sauvegarde, mais aussi du contrôle de l'accès et de toute la sécurisation, ce qui constitue une aide évidemment précieuse. Mais n'oubliez pas que vous devez organiser personnellement l'accès à votre PC personnel et/ou à votre réseau. Cette tâche, nombre de confrères la confient – à juste titre – à une entreprise extérieure. À cet égard, il est essentiel d'établir un contrat qui non seulement décrit les activités prévues, mais impose également une obligation de résultat. Il ne peut évidemment pas être question d'« usage normal », pas plus que de faire « de son mieux », formulations qui ne permettent pas de garantir une protection à 100 %.

Il est recommandé d'installer un *hardware firewall* (matériel pare-feu). Il s'agit d'un appareil, équipé d'un logiciel, qui régule l'accès via Internet (ADSL ou câble) avant que l'information arrive sur votre (vos) ordinateur(s).

Il est en outre indispensable d'installer un *software firewall* (logiciel pare-feu), qui bloque les intrusions dans votre système au départ d'informations plus précises et actuelles.

Les droits d'accès aux répertoires et fichiers sont à fixer dans chaque bureau en particulier, éventuellement en concertation avec un responsable réseau. Une tâche que vous pouvez également sous-traiter.

De votre côté, vous pouvez veiller à définir les paramètres via les propriétés des fichiers. Vous pouvez le faire via l'onglet « Partager » ou « Partager fichiers ». Cela n'a rien de compliqué et, moyennant un travail expérimental, vous pouvez vérifier, au départ d'un autre ordinateur de votre réseau, si les droits attribués sont suffisants.

Néanmoins, les principales menaces se situent le plus souvent à un autre niveau. Chaque jour, les *spams* et virus affectent la vie professionnelle des experts-comptables et conseils fiscaux. Souvent même, ils sont source de stress et d'irritation. À juste titre, d'ailleurs ! Les menaces sont nombreuses et proviennent de partout. En voici les principales :

- *Spam* désigne les *e-mails* indésirables envoyés en vrac ou en masse.
- *Malware* désigne toute forme de logiciel malveillant ou dommageable.

- *Spyware* désigne toute forme de logiciel qui utilise votre connexion à Internet pour collecter et envoyer des données.
- *Adware* désigne tout logiciel qui fait apparaître des annonces publicitaires sur votre écran et qui, éventuellement, utilise votre connexion à Internet pour envoyer des données.
- *Browser hijacker* désigne tout logiciel malveillant qui modifie les paramètres de votre navigateur Internet, notamment la page de démarrage, les barres d'icones, etc.
- *Phishing* désigne toute forme criminelle de vol d'identité par voie électronique, notamment par le biais d'annonces publicitaires ou d'*e-mails* de banques internationales, etc.
- *Cheval de Troie* désigne tout petit fichier qui s'installe sur votre disque dur par le biais d'*e-mails* ou de programmes gratuits ou qui y est directement enregistré par un pirate informatique, et qui s'y « niche » pour ensuite continuer à se répandre. Les chevaux de Troie peuvent affecter les données ou fichiers-programmes ou en détruire certaines parties.
- *Virus* désigne tout programme qui s'installe sur votre disque dur et se propage spontanément avec des intentions malveillantes, notamment celle de détruire ou de rendre inutilisables certains fichiers ou parties de fichiers.
- *Hacker* désigne toute personne qui accède à votre ordinateur à votre insu et dont les intentions peuvent être tantôt innocentes, tantôt criminelles.

Pour une description détaillée de ces menaces et pour une protection efficace contre celles-ci, nous vous renvoyons aux entreprises et ouvrages spécialisés en la matière. À cet égard, il est essentiel que vous fassiez le nécessaire au sein de votre bureau afin d'écarter toute forme de menace. À cette fin, il vous faudra acquérir divers logiciels, qui pourront – dans la mesure du possible – être couplés, sachant qu'il n'est pas rare que les logiciels de sécurisation provoquent des conflits. Il est dès lors indispensable que vous soyez bien informé.

Il est également important que vous portiez un regard critique sur l'organisation des copies de sauvegarde. Il ne peut être admis ni possible qu'une copie de sauvegarde de fichiers (potentiellement) infectés de virus, chevaux de Troie, *malwares*, etc., soit réalisée. Vous devez donc faire preuve de prudence à cet égard.

Enfin, nous aimerions attirer votre attention sur les principes suivants, lesquels sont applicables en matière de sécurisation informatique, à savoir :

- l'emplacement le plus difficile à sécuriser est le dernier mètre ;
- le matériel le plus difficile à sécuriser est le matériel mobile.

Le premier principe fait référence à la distance entre notre cerveau ou nos mains et notre PC proprement dit. Nous pouvons en effet parer toute forme de menace en la contournant ou en la neutralisant personnellement. Il est recommandé d'en tenir compte lors de l'installation ou de la maintenance de vos programmes de sécurisation.

Même vos collaborateurs les plus proches peuvent autoriser l'accès de *malwares* indésirables pour votre système par le biais de disquettes, de *memory sticks* USB, etc., ou copier des programmes ou données dans votre système. Vous devez donc fixer des règles claires concernant l'utilisation des mémoires externes ainsi que de la connexion par câble ou WIFI (*wireless Internet*) d'ordinateurs portables, PDA, smartphones, etc. Ces derniers présentent en effet les plus gros foyers d'infection.

Le ministre Marc Verwilghen a récemment inauguré un site Internet pratique qui offre toutes les armes pour parer aux dangers d'Internet et de ses menaces, à savoir http://www.spamsquad.be. Nous ne pouvons que vous conseiller de consulter ce site avec la plus grande attention.

Conclusion

Il existe diverses possibilités de réaliser un *scanning* en ligne gratuit pour rechercher les virus, logiciels espions, etc.

Il est en tout cas conseillé d'installer un bon antivirus/antilogiciels espions et de faire contrôler régulièrement vos disques fixes et amovibles.

Il est essentiel que vous soyez prudent et que vous évitiez de consulter arbitrairement toutes sortes de sites Internet douteux, de télécharger et d'installer des logiciels inconnus, d'ouvrir et de lire des *e-mails* suspects. Car, en fin de compte, c'est vous qui ouvrez la porte à la plupart des infections...

Bonne chance ! ●