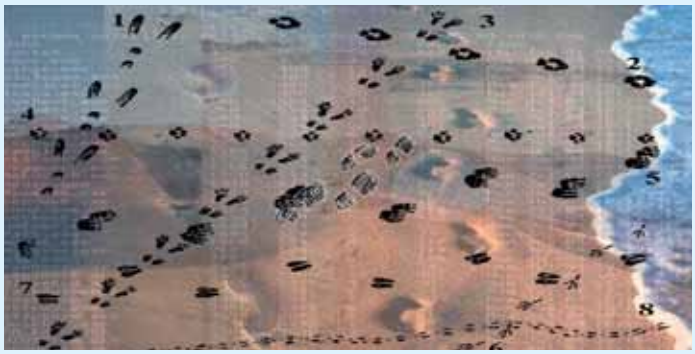
Un PC transparent

Thomas Engel (photo: màd)

Nous laissons toujours plus de «traces» de notre passage. A côté des cartes de crédit, des cartes Cumulus et SuperCard, du téléphone portable ou de la carte santé, bon nombre des programmes que nous utilisons tous les jours laissent «traîner» des données numériques derrière eux. Nous ne saurons jamais tout ce qui va et vient, entre et sort par le web. Souvent, des programmes s'annoncent à leur fabricant chaque fois que l'on s'en sert, envoient des indications de versions et d'enregistrement, et parfois bien d'autres choses encore!

A ceci s'ajoutent encore des «hôtes» indésirables déguisés en petits auxiliaires bien intentionnés, mais qui jettent des regards curieux sur nos données bancaires, mots de passe et autres contenus intéressants de nos ordinateurs. Les pirates informatiques *(hackers)* qui les ont envoyés reçoivent ainsi à domicile d'innombrables données, gratuitement de surcroît. Ces «hôtes», ce sont des chevaux de Troie *(Trojans)* ou des virus qui, malheureusement, deviennent toujours plus professionnels, toujours plus nombreux et toujours plus malins.



Tous ceux d'entre nous qui gèrent des données sensibles sur leur ordinateur ou qui effectuent des transactions bancaires en ligne se doivent d'attacher la plus grande importance à cet aspect. De plus en plus de médecins dentistes ont «informatisé» leur cabinet dentaire au cours de ces dernières années. Ils gèrent de la sorte des centaines de données de leurs patients sur leurs serveurs et traitent souvent leurs affaires bancaires via Internet. Ils deviennent ainsi des proies de rêve pour maints gangsters du net, et le cauchemar de tout protecteur des données. Les directives applicables sont très strictes et ne laissent aucune marge de manœuvre lorsque l'on travaille avec des données numériques sensibles. Nombre de nos actions au jour le jour risquent ainsi d'être problématiques à la lumière de la protection des données, voire même illégales.

Que peut-on faire?

Le plus simple et le plus sûr, c'est d'isoler l'ordinateur de l'Internet et de ne plus jamais l'y reconnecter. Malheureusement, cette option n'est plus guère praticable de nos jours. On pourrait aussi utiliser des systèmes séparés: un PC pour toutes les activités sur l'Internet, un autre complètement séparé pour toutes les données de nos patients. Malheureusement, le PC «isolé» devra tout de même se connecter de temps à autre à Internet, ne serait-ce par exemple que pour des mises à jour ou pour des activités de maintenance. En effet, de plus en plus de fournisseurs de logiciels et de matériels exigent une connexion Internet pour intervenir. Que peut-on donc faire pour minimiser les risques? Il faut considérer plusieurs aspects: le système d'exploitation doit être tenu à jour (mises à jour de sécurité!); il faut disposer d'un programme anti-virus efficace; le navigateur doit être actuel et sa mémoire cache doit être périodiquement vidée; les mots de passe doivent être périodiquement changés. Au sujet des mots de passe: ils doivent avoir au moins huit à dix caractères, contenir des lettres majuscules et minuscules ainsi que des caractères spéciaux et des chiffres. On peut faire examiner un mot de passe de ce type (mais pas le vrai!) à l'adresse https://passwortcheck.datenschutz.ch/. Un autre élément important est à prendre en considération si ce message s'affiche à l'écran lorsque l'on se renseigne auprès de Microsoft: *Utilisez dès maintenant un pare-feu. En cas de précautions insuffisantes, les liaisons Internet peuvent présenter divers risques. Un pare-feu permet de limiter ces risques.*

Pare-feu (*Firewall* en anglais)

Qu'est-ce qu'un pare-feu? Pour l'expliquer, je vais simplifier et illustrer rapidement ce qu'est le trafic sur Internet: le WWW, c'est comme un immense réseau routier qui sert à transporter d'innombrables paquets de données. Chaque PC dispose de plusieurs accès au réseau par lesquels ces paquets peuvent entrer et sortir, comme un point de franchissement frontalier d'un pays à un autre. En fonction du système d'exploitation et du type d'ordinateur, on peut avoir plus de 65 000 de ces «points de passage», nommés *«ports»* en langage informatique. En Suisse, ce sont les gardes-frontière qui les surveillent. Sur un PC, il n'y a personne pour s'en charger et les paquets de données peuvent librement aller et venir. Un pare-feu, c'est en quelque sorte un garde-frontière pour PC qui se charge de la surveillance de ces *ports.* Il existe plusieurs systèmes de pare-feu qui se différencient en fonction de leur degré de sécurité et de leur infrastructure. On peut, pour généraliser, les répartir en catégories matériel ou logiciel, interne ou externe. Pour ne pas remplir des dizaines de pages, je ne vais pas décrire les pare-feu logiciels personnels: il y a aujourd'hui de nombreux fournisseurs de ces produits. Ils vont du gratuit au très cher, en fonction des besoins et de l'étendue des équipements à protéger. Celui qui voudra protéger son cabinet dentaire par un pare-feu devrait s'adresser à un informaticien expérimenté. Pour protéger un PC privé, des logiciels simples suffisent comme, par exemple: Zone Alarm Pro, Kerio Firewall, Outpost Pro, Kaspersky Anti Hacker Firewall, McAfee Personal Firewall, et bien d'autres encore.

Ce n'est qu'en surveillant nos *ports* que l'on s'aperçoit à quel point sont nombreux les programmes qui échangent des données via Internet, et à quelle fréquence. Selon le pare-feu utilisé, ont peut accorder des droits de passage spécifiques à chaque port et à chaque programme. Le passage peut être toujours autorisé, toujours interdit, ou autorisé après demande. Certains pare-feu précisent quels sont les services auxquels on peut faire confiance, identifient les autres et les bloquent. Souvent, les pare-feu travaillent étroitement avec l'anti-virus, ou bien ils y sont même intégrés. Selon le niveau de sécurité, le pare-feu peut aller jusqu'à paralyser le PC et bloquer tout trafic Internet. La règle d'or, c'est toujours de choisir le bon programme et les bons réglages.

A suivre…