Cryptage des données

Thomas Engel (texte et photo)

Nos ordinateurs personnels ne cessent d'exporter des données, que ce soit via des courriels, via FDP, en les gravant sur un CD, en les enregistrant sur une clé USB ou sur internet. Hélas, ces données ne finissent pas toujours entre les mains de leurs destinataires légitimes. Elles se perdent, sont volées ou bien espionnées au passage.

J'ai déjà évoqué dans plusieurs articles la question de la sécurité des données dans la perspective de leur sauvegarde. Malheureusement, j'apprends trop souvent que des gens ont perdu leurs images, textes, etc. à la suite d'un crash de leur disque dur ou de la perte de leur laptop. Le sujet de la sécurité des données en termes de leur protection est donc d'une toute autre nature. Nous autres médecins-dentistes travaillons avec les données personnelles de nos patients, et c'est pourquoi leur sécurité doit nous tenir à cœur. Les clés USB ont désormais des capacités élevées de 32, 64, voire 128 GB, ce qui leur permet de stocker des quantités incroyables de données. Il est très facile d'avoir toujours avec soi la totalité des photos et données de notre cabinet dentaire sur une seule clé USB. Mais si nous la perdons, si elle nous est dérobée, alors nous perdons le contrôle sur ces données. Il existe aujourd'hui des programmes spécifiques pour leur cryptage. Ils les stockent dans des sortes de *volumes* de données et rendent pratiquement impossible d'y accéder sans le mot de passe *ad hoc.* En cas de perte du support qui tomberait en de mauvaises mains, nous pouvons être relativement assurés que nos données ne pourront pas être lues. Et puis nous serons protégés de toutes conséquences en droit tant que nous pourrons rendre crédible que nos données sensibles étaient bel et bien cryptées.

TrueCrypt par exemple est un programme de cryptage gratuit. Il tourne aussi bien sous Windows que Mac et Linux.

Cryptage

AES: Advanced Encryption Standard. C'est une norme de cryptage symétrique, ce qui signifie que le même mot de passe est utilisé au cryptage et au décryptage.

Le logarithme d'AES peut s'appliquer avec des blocs de 128 bits et une clé dont la longueur peut être de 128, 192 ou 256 bits. Il offre une sécurité élevée et peut être utilisé sans frais de licence car son algorithme est libre. Les données sont découpées en blocs lors du cryptage, et chaque bloc est crypté séparément et passe par plusieurs cycles ou rondes de cryptage.

Twofish: c'est également un algorithme symétrique qui est appliqué pour le cryptage en blocs de 128 bits et 16 rondes. Les longueurs de clé sont de 128, 192 ou 256 bits.

Comme dans le cas du cryptage AES, chaque bloc est crypté en plusieurs rondes XOR réciproques.

Serpent: c'est une méthode de cryptage considérée très sûre, mais relativement lente, raison pour laquelle elle est souvent utilisée par les technologies de cryptage reposant sur le matériel plutôt que sur le logiciel.

TrueCrypt inclut les trois types de cryptage et peut les combiner entre eux. Il existe encore bien d'autres programmes de cryptage, mais *Twofish, Serpent* et *TrueCrypt* comptent parmi les plus connus et les plus sûrs. C'est pourquoi ils sont très souvent utilisés.

Il existe des mémoires de masse en ligne qui cryptent les données lors de leur enregistrement et les protègent ainsi de tout accès non autorisé. L'une d'entre elles fait partie du service «Wuala» développé par l'Ecole polytechnique fédérale.

Points faibles

Ces programmes sont si sûrs que l'on n'a pas connaissance que des attaques aient réussi à ce jour. C'est l'utilisateur lui-même qui présente le plus grand de tous les risques! En effet, le meilleur des programmes de cryptage ne sert absolument à rien si le mot de passe est trop faible ou s'il est inscrit quelque part. C'est pourquoi la plupart des attaques dont on a eu connaissance et qui ont réussi visaient les mots de passe qui, une fois volés, permettent de décrypter les données.

Il existe aujourd'hui de très nombreux programmes d'espionnage dont le seul but est d'enregistrer chaque frappe sur le clavier et de communiquer la séquence à «l'espion».

Si le logiciel de cryptage n'est pas mis à jour, il ne sera plus disponible avec un nouveau système d'exploitation, et l'on ne pourra plus accéder aux données cryptées sur l'ancien système.

Autre danger: la perte du mot de passe. Le cryptage des données est en effet si sûr qu'il sera impossible d'y accéder à nouveau sans disposer du mot de passe correspondant.

A suivre…