Le retour de la stéganographie, pour dissimuler sans attirer l'attention

- Informatique - Sécurité Informatique -

Date de mise en ligne : jeudi 5 juin 2008

Spyworld Actu

La « stéganographie » est le complément de la cryptographie. Elle protège les fichiers secrets au même titre que la cryptographie protège les fichiers confidentiels. Voici les principes de base et deux logiciels opérationnels pour la mettre en oeuvre.

La stéganographie a été inventée par les grecs pour cacher des informations. Le mot stéganographie vient du grec « steganos » qui veut dire « caché » dans le sens de « enfoui », comme un sous-marin. Le mot Grec « crypto » veut dire également « caché » mais dans le sens où « on ne comprend pas la signification ». Deux mots de Grec donc pour deux modes de traitement des informations, distincts et complémentaires.

La cryptographie au temps de César

Que faire pour protéger des documents confidentiels dans son entreprise ? La seule réponse actuelle est le chiffrement, la « crypto ». Les Romains ont largement utilisé cette technique lors de la guerre des Gaules avec le code « 3 » de Jules César. On chiffre le message avec une clé et on transmet la clé à tous les destinataires. En cas d'interception, le message ne pourra pas être lu. Par exemple, le message chiffré sera « DAH » et la clé « 3 ». Le message en clair sera donc « AVE », « D-3=A » et ainsi de suite. En décalant de trois caractères la lettre d'origine on obtient le message en clair. Aujourd'hui toute la protection des données sensibles, repose sur le même principe, avec bien évidemment des algorithmes plus complexes.

Ne pas attirer l'attention grâce à la stéganographie

Le problème est, qu'une donnée cryptée attire l'attention dans une masse de données en clair. Il est évident pour un hacker ou une puissance étrangère que les données chiffrées sont les données les plus « intéressantes ». Il faut donc appliquer une autre stratégie pour les données « secrètes » qui ne doivent pas attirer l'attention. La stéganographie moderne utilise un programme qui va encapsuler le fichier secret à protéger dans un autre fichier dit « hôte », plus grand, et qui sera anodin comme une photo ou une musique. Ce logiciel rend le fichier « secret » totalement invisible et perdu dans la masse de fichiers « en clair ».

Facilite la fuite d'informations en entreprise

Plusieurs avantages à cette technique. Lors de la perte d'un ordinateur portable, les fichiers sensibles ne seront pas visibles par le voleur. Les douanes et autres systèmes de scan qui se concentrent sur les fichiers cryptés ne verront pas ces contenus. Des données secrètes au niveau même de l'entreprise ne seront pas visibles par d'autres personnes que celles au courant de l'existence du fichier. Même les informaticiens ne seront pas au courant et ne pourront pas les lire. Quelques inconvénients : Au niveau de la sécurité d'un pays, tous les délinquants peuvent utiliser ces techniques pour éviter d'être interceptés. De plus, en entreprise, les fuites d'informations à travers l'envoi d'un email sont facilitées pour les personnels indélicats.

Deux outils intéressants

Il faut donc connaître ces techniques et les expliquer aux dirigeants des entreprises. « Un secret n'existe pas, sinon ce n'est plus un secret ... », comme disent les militaires. De quels programmes dispose-t-on pour mettre en oeuvre la stéganographie ? Deux sont intéressants : Invisible Secrets 4, un shareware Roumain, donc européen et Truecrypt un logiciel gratuit qui permet de cacher un volume virtuel d'un disque dur, lui-même crypté.

http://www.truecrypt.org/docs/?s=hi... Grâce à de tels outils, on peut cacher un fichier dans une image. On ne verra alors aucune différence à l'oeil nu entre l'image « hôte » et l'image contenant le fichier caché. La différence est dans le contenu du fichier, et dans la « vraie vie » le fichier d'origine n'étant pas disponible, il faut d'abord trouver quel fichier parmi des centaines de milliers, contient l'information stéganographiée. On peut éventuellement renforcer la sécurité en combinant la stéganographie avec un chiffrement à l'intérieur du fichier.

Post-scriptum :

http://securite.reseaux-telecoms.ne...