Précautions lors des déplacements en mission

Lors des déplacements à l'étranger, des risques et des menaces pèsent sur la sécurité des informations. Les informations emportées ou échangées peuvent attirer des convoitises de toute sorte. Il convient donc de veiller sur leur sécurité et notamment sur leur confidentialité. Les cybercafés, les hôtels, les lieux publics et parfois même les bureaux de passage peuvent être des lieux à risques. Dans de nombreux pays étrangers, les centres d'affaires et les réseaux téléphoniques sont surveillés. Dans certains, les chambres d'hôtel peuvent être fouillées.

L'agence nationale pour la sécurité des systèmes d'information (ANSSI) nous invite à suivre les conseils qu'elle a élaborés dans son guide de recommandations intitulé : « passeport de conseils aux voyageurs ». Il convient d'adopter quatre attitudes :

- avant de partir en mission.
- pendant la mission.
- avant le retour de mission.
- après la mission.

En voici quelques extraits :

Avant de partir en mission

1. Relire attentivement et respecter les règles de sécurité édictées par son organisme.
2. Prendre connaissance de la législation locale.
3. Utiliser de préférence du matériel dédié aux missions (ordinateurs, téléphones, supports amovibles, etc.).
4. Sauvegarder les données que l'on emporte.
5. Éviter de partir avec des données sensibles.

Pendant la mission

1. Garder ses appareils, supports et fichiers avec soi.
2. S'il faut se séparer de son téléphone portable, retirer et conserver avec soi la carte SIM ainsi que la batterie.
3. Utiliser un logiciel de chiffrement conforme aux réglementations locales pendant le voyage.

Attention aux échanges de documents (par exemple : clé USB lors de présentations commerciales ou lors de colloques). Ne pas utiliser les équipements qui sont offerts. Emporter une clé destinée à ces échanges et effacer les fichiers, de préférence avec un logiciel d'effacement sécurisé.

Avant le retour de mission

1. Transférer ses données sur le réseau de son organisme à l'aide d'une connexion sécurisée, ou sinon sur une boite de messagerie en ligne dédiée à recevoir les fichiers chiffrés. Les effacer ensuite de sa machine, si possible de façon sécurisée, avec un logiciel prévu à cet effet.
2. Effacer l'historique des appels et de la navigation.

Après la mission

Changer les mots de passe utilisés pendant le voyage, analyser ou faire analyser son équipement. Ne pas connecter ses appareils au réseau avant d'avoir fait au minimum un test anti-virus et anti-espiogiciels.

Voir le document complet édité par l'ANSSI :
http://wiki-si.ias.u-psud.fr/redmine/attachments/13/Passeport-de-conseils-aux-voyageurs_janvier-2010.pdf