CTP Sécurité des systèmes d'information - DOM du 19 juin 2008

Plan de l'intervention RSSI

Il n'est pas inutile de rappeler brièvement dans quel esprit la SSI s'est mise en place à l'Insee.

1- Ré affirmer les principes fondateurs de la SSI :

Nous prenons une responsabilité vis à vis des citoyens et des entreprises en collectant des données individuelles. Celle de protéger ces données de tout regard non autorisé : en interne, bien sûr, mais surtout de l'extérieur.
C'est une responsabilité qui est inscrite dans la loi, bien sûr, et nous avons l'obligation de nous y soumettre.
Mais une deuxième dimension est fondamentale : celle de la confiance que nous font les citoyens et les entreprises dans la gestion des données qu'ils nous confient.
Cette confiance nous sonne des responsabilités, que nous avons évoqué souvent en CTP. C'est de nous opposer à ce qu'un gouvernement, quel qu'il soit, n'utilise des données détenues par l'Insee pour léser des droits fondamentaux des individus. D'où notre ferme opposition à l'implication de l'Insee dans la validation des données d'État-Civil comme l'avait prévu le projet Inès de carte d'identité informatisée, ou à toute extension du champ d'utilisation du NIR.

2- Pas de SSI sans adhésion du personnel à ses principes

Ce qui signifie :

- sans donner les clés techniques des systèmes de protection, bien sûr, il faut donner la maximum d'information à chaque agent sur le système de protection mis en place et sur ses finalités. De ce point de vue, la routine est sans doute la pire ennemie de la sécurité. Il faut réfléchir en permanence à l'animation de cette dimension et surtout ne pas confiner la question de la sécurité dans un petit cénacle de spécialistes, comme c'est parfois le cas dans les établissements ;
- obtenir un consensus sur les principes de la sécurité. Sans entamer de polémique, deux exemples : le système d'accès physique à MK1 et MK2 et les heurts qui se sont produits avec les fumeurs sont négatifs : un système de sécurité incompréhensible ne peut fonctionner. La mise en place du cryptage sur les micros portables CAPI s'est accompagné de dysfonctionnements importants qui ont pénalisé les enquêteurs ;
- que les règles édictées ne soient pas d'autant plus mal appliquées ou même violées que l'on est en haut de la hiérarchie. Nous faisons allusion par exemple à la demande de mots de passe par des supérieurs hiérarchiques, dont nous avons de nouveaux exemples tous les ans.
- La proportionnalité de la protection à l'utilité de la protection est fondamentale. Deux exemples : interdire la mail pour les contacts avec les entreprises pour Esane, alors même que les échanges n'auraient aucun caractère de véritable confidentialité nous paraît peu justifié, au vu des conséquences démesurées sur le travail des gestionnaires ; Protéger des données, c'est bien, les perdre par fragilité technique ou défaut d'archivage n'est pas un facteur de mobilisation sur ces questions (cf IPCR). Intervenir en maintenance sur le bunker sécurisé du CNIP sans pouvoir accéder aux éléments permettant de repérer la panne ne simplifie pas la vie.

Questions :

- ouverture de la messagerie aux nomades : pour quelques exceptions, ou pour toutes et tous ? Où et quand les principes seront-ils explicités ?
- complexifier le mot de passe : oui, mais combien de petits papiers scotchés sur les écrans ou dans le premier tiroir du bureau pour s'en souvenir ?
- sur les Intranet d'établissement, restriction croissante dans l'accès aux notes. On a le sentiment qu'il y a une escalade pour classifier en protection les notes, sans utilité. Nous sortons d'une époque où l'opacité devenait la règle et l'information l'exception. Ce qui a deux inconvénients : la sécurité est banalisée, et tout débat sur le niveau de sécurité à affecter à une information interne disparaît.