Bordeaux-Mérignac, mercredi 5 décembre 2012

Garçon ! CssIP avec un peu de SSI siouplaît …

Il y a près de deux années, nous nous étions inquiétés de l'absence de prise en compte de la « Sécurité des Systèmes d'Information » par la Direction des Services de la Navigation Aérienne au regard des exigences qu'elle aurait dû formuler et des moyens qu'elle devrait engager (organisation, outils, formation, etc) :

RENAR-IP... Y a-t-il un pilote dans l'avion ? (10 février 2011)

À la veille de la mise en service :

- aucun contour de défini sur l'arbitrage et la criticité des incidents
- les outils de supervision et d'administration sont inadaptés
- pas de réelle prise en compte de la sécurité et de la sûreté
- les superviseurs ne sont pas encore formés et n'ont pas de Plan de Formation établi

Rappelons l'attitude adoptée par la direction au travers de cet extrait d'un document phare remis en réunion de conciliation aux organisations syndicales :

Renforcement de l'armement de la supervision

Question (des OS) :

- L'augmentation de la charge de travail, l'augmentation des responsabilités et la prise en compte des aspects SSI nécessitent la mise en place d'un 2eme superviseur réseaux H24.

Réponses (du DSNA) :

- La **très bonne fiabilité des équipements et des liaisons de nouvelle génération** devrait assurer un haut niveau de disponibilité du réseau.
- La possibilité d'une évolution de l'armement de la supervision vers un 2eme superviseur réseaux H24 sera analysée par un groupe de travail local en fonction du retour d'expérience et de l'évolution du partage des tâches entre la supervision opérationnelle et la maintenance spécialisée.

Pour ce qui est du retour d'expérience, nous donnons acte qu'à ce jour nous avons eu connaissance d'aucune attaque SSI sur le nouveau réseau opérationnel de la navigation aérienne.

Dans le relevé de conclusions de sortie du conflit social au CESNAC, Monsieur le Directeur des Services de la Navigation Aérienne nous a lui-même donné sa dernière position :

Dans le domaine SSI, les fonctions de routage du réseau ne sont plus présentes dans les sites isolés (stations radar et antennes avancées) ce qui limite de manière très significative les possibilités d'attaque. Les conséquences seraient en tout état de cause de rendre indisponible le service sur ce seul site isolé.

Pour résumer, le discours aux organisations syndicales a été systématiquement d'affirmer que la SSI n'était pas un enjeu majeur pour CssIP. Cette réponse ne nous a jamais satisfaite ; mais, à partir de cette prise de position de la direction, nous n'avions effectivement plus de raison objective de poursuivre un tel conflit (mais sans pour autant être convaincus).

Il semble que d'autres spécialistes de la DSNA externes au CESNAC réunis en GT ont rejoint notre position. Ceux-ci s'inquiètent également de l'absence de mise en place d'un personnel *en ligne* avec le niveau de compétence approprié pour gérer un événement SSI sur le nouveau réseau.

Récemment, au travers d'un communiqué, le DSNA a apparemment infléchi sa position en prônant une sensibilisation du personnel aux aspects SSI. C'est une avancée significative. Mais nous déplorons que cette nouvelle orientation n'ait pas été présentée aux organisations syndicales, que les plans de formation des personnels ne soient pas à jour et qu'aucune discussion avec les experts locaux n'ait eu lieu.

L'organisation de cette sensibilisation est étonnante :

- Une formation graduée suivant trois niveaux, mais aucun de ces niveaux ne semble correspondre à un objectif sérieux de qualification. Quelques uns de nos collègues (peu nombreux) travaillant depuis de longues années dans ce domaine très particulier ont déjà pu les éprouver et, à l'aune des formations proposées, ces derniers nous affirment que leur propre niveau de formation doit se situer entre 10 et 20…
- Le personnel ciblé pour les différents niveaux de formation n'est pas forcément en adéquation avec la réalité. La disponibilité des systèmes étant l'objectif probable d'une attaque éventuelle au travers d'un réseau, le DSNA exclut les superviseurs en charge des systèmes du même niveau de sensibilisation que ceux en charge des réseaux.
- Enfin, rien n'est prévu sur le maintien des compétences.

D'évidence, il ne s'agit là que de formation prétexte à nous faire estampiller sur le bas du dos un pseudo label SSI. Est-il encore besoin de rajouter quelques chose sur le crédit d'une telle action ?

Un peu de technique :

La DSNA, pourtant consciente que le cœur de notre réseau (ou *backbone*) transite dans l'espace public, ne s'émeut pas que les données opérationnelles circulant entre les sites soient laissées en libre accès à quiconque, avec une formation réseau tout à fait classique, pourra se brancher sur un des nombreux points de présence de l'opérateur à l'aide d'un analyseur de réseau (matériel très répandu, sauf à la DSNA). Mais la DSNA compte sur « *La très bonne fiabilité des équipements et des liaisons de nouvelle génération* » pour « *assurer un haut niveau de disponibilité du réseau* ».

Nous sommes persuadés que des réponses raisonnables et satisfaisantes peuvent être trouvées : elles se situeront entre le mieux disant attendu de la majorité des experts et le refus de la direction depuis le début de considérer la SSI comme un enjeu majeur. Mais, ces réponses ne verront pas le jour tant que l'affichage d'une politique sans réelle consistance sera le seul objectif du DSNA.

Quelle est l'exigence de sécurité et de sûreté voulue ? Quelle est la taille des effectifs concernés ? Le cas échéant, comment développer ces nouvelles compétences qui ne sont maîtrisées aujourd'hui que par un tout petit nombre d'experts ? Pourquoi l'expertise actuelle n'est pas reconnue et comment la faire reconnaître ?

Voilà quelques exemples de question à se poser.

Nous ne nous laisserons pas embarquer dans une telle situation, ni être complice de cette attitude se limitant à demander à l'encadrement intermédiaire de mettre des croix dans nos tableaux de formation.

Les IESSA du CESNAC réunis en intersyndicale