Section CRNA-Est

14/01/2022

Alerte Cyber au CRNA-Est

La section UNSA-IESSA du CRNA-Est dénonce les risques que l'absence de stratégie nationale sur la cybersécurité fait courir aux IESSA.

La menace d'une attaque informatique est bien réelle et se renforce même de jour en jour. Comme le disait le Directeur Général de l'Aviation Civile la semaine dernière, après que nous l'ayons interpellé sur ce sujet lors de sa visite au CRNA-Est, la question n'est pas de savoir si mais quand la DSNA sera l'objet d'une cyberattaque.

Si cela est inéluctable, qu'attend donc notre administration pour agir, investir et communiquer ? Nous déplorons le fait que l'encadrement local et les IESSA du service technique soient des victimes collatérales de cette inaction.

A l'analyse des documents de référence PSSI DGAC 2018 niv-2 et niv-3, il est temps que tout le monde prenne conscience de la réalité :

- Nous IESSA sommes les seuls à avoir en charge les systèmes techniques les plus critiques (classés noir ou rouge au sens PSSI) et donc à assurer leur sécurité.
- En tant qu'administrateurs de ces systèmes (c'est-à-dire ceux qui détiennent le mot de passe administrateur), nous avons des responsabilités qui nous engagent judiciairement.
- En cas d'incident, des procédures d'urgence doivent prévoir l'isolement et la reconfiguration des systèmes opérationnels. Ces procédures doivent faire l'objet de formation et d'entraînement. Rien de tel n'existe au CRNA-Est.
- En cas d'intrusion sur un système opérationnel, les superviseurs doivent en alerter le SOC, qui lui est à horaire de bureau. Espérons que les pirates informatiques le soient aussi …

La question du jour …

Qui prendra la décision d'arrêter les serveurs 4Flight en cas d'incident cyber ?

(Les superviseurs ? L'IAT ? le Chef de Centre ? le DSNA ? le DGAC ? Le Ministre ?)

« Le non-respect des exigences de la PSSI peut donner lieu à des mesures disciplinaires, voire pénales (compromission d'informations protégées). » cf. « PSSI DGAC 2018 - Niv-3 - V1R2 » - Introduction.

A l'horizon 4Flight, nous demandons à l'administration de bien jauger les risques alors qu'elle sollicite les IESSA pour la mise en œuvre d'interconnexions entre l'opérationnel et Internet.

La section UNSA-IESSA prendra donc toutes les initiatives qu'elle jugera nécessaires afin de protéger nos collègues. Ce qui est certain, c'est qu'en cas d'incident cyber, ce seront les IESSA experts et superviseurs qui devront répondre aux questions du juge.