ONZIÈME CONFÉRENCE DE NAVIGATION AÉRIENNE

Montréal, 22 septembre – 3 octobre 2003

Point 2 : La sécurité et la sûreté dans la gestion du trafic aérien (ATM)
2.5 : Sécurité et sûreté de l'infrastructure ATM

METHODOLOGIE DE SURETE INFORMATIQUE POUR LES RESEAUX OPERATIONNELS DE LA NAVIGATION AERIENNE FRANÇAISE

(Note présentée par la France)

SOMMAIRE

Aujourd'hui, les systèmes informatiques ont pris une place majeure au sein de la Navigation Aérienne, et la sécurité et la sûreté des systèmes informatiques est un facteur essentiel pour l'accomplissement des missions pour les services de la Navigation Aérienne.

Cette note de travail a pour objet de présenter la méthodologie qui a été retenue par la Navigation Aérienne française pour prendre en compte la problématique de sûreté informatique de son Système d'Information opérationnel.

Les propositions d'actions pour la conférence sont au paragraphe 5.

1. HISTORIQUE ET PROBLEMATIQUE DE LA SURETE ET DE LA SECURITE INFORMATIQUE POUR LA NAVIGATION AERIENNE FRANÇAISE

1.1 La préservation de la sécurité d'un Système d'Information (SI) peut se définir par le maintien de sa disponibilité, de son intégrité et de sa confidentialité. La sûreté, qui peut être considérée comme un sous-ensemble de la sécurité du Système d'Information, a pour objectif particulier de veiller à protéger la sécurité du Système d'Information vis à vis d'atteintes malveillantes.

Aujourd'hui, les systèmes informatiques ont pris une place majeure au sein de la navigation aérienne, et la sécurité et la sûreté du Système d'Information sont des facteurs essentiels pour l'accomplissement des missions pour les services de la navigation aérienne.

Il y a encore quelques années, le Système d'Information de la navigation aérienne était un système clos, n'offrant pas ou très peu d'interactions avec l'extérieur. L'exposition aux menaces vis-à-vis de sa sûreté pouvaient être considérée comme faible, du simple fait qu'il était difficile d'atteindre le Système d'Information, par des moyens logiques, depuis un point d'accès extérieur à celui-ci. La prise en compte de la **sûreté** pouvait dès lors se limiter à protéger les accès physiques au Système d'Information.

1.2 Cependant, depuis plusieurs années, on observe que, dans le même temps que s'affirme l'importance du Système d'Information pour les missions de la navigation aérienne, la complexité de ce système s'accroît, et il évolue vers un système de plus en plus interconnecté avec d'autres systèmes, d'autres réseaux, dont le contrôle échappe à la navigation aérienne. Ces interconnexions sont dictées par la nécessité d'interactions, et d'échanges de données avec les partenaires de la navigation aérienne (partenaires européens, exploitants aériens…). Dans le même temps, les technologies «propriétaires» cèdent peu à peu le pas aux technologies standards, telles que le protocole IP (Internet Protocol) pour les réseaux, ou UNIX pour les systèmes d'exploitation.

L'ensemble de ces facteurs accroît la sensibilité du Système d'Information et augmente le risque d'exposition aux menaces externes. Le risque d'atteinte à la sûreté de ce Système d'Information de la part de personnes malveillantes s'accroît donc de façon significative.

1.3 Au vu de ce constat, il est donc apparu clairement à la Direction de la Navigation Aérienne française qu'il était nécessaire de prendre en compte de façon plus approfondie, la problématique du maintien de la sécurité et de la sûreté de son Système d'Information, et, en particulier, les problèmes de protection vis-à-vis des menaces logiques d'origine externe.

2. METHODE DE PRISE EN COMPTE DE LA PROBLEMATIQUE

2.1 Pour pouvoir abaisser le niveau des risques pesant sur le Système d'Information à un niveau acceptable, il est nécessaire de définir des mesures de protection techniques, organisationnelles ou procédurales, à même de corriger les vulnérabilités du Système d'Information. Ces mesures doivent être définies au moyen de règles, qui doivent :

- Couvrir la problématique de façon exhaustive;
- Définir des mesures de protection homogènes;
- Définir des mesures de protection applicables, reconnues et effectivement appliquées.

2.1.1 Être exhaustif signifie couvrir tous les aspects pouvant impacter la sûreté, c'est à dire : les interconnexions du Système Informatique avec l'extérieur, les interconnexions internes au Système Informatique (entre sites), l'utilisation, l'exploitation et la maintenance des équipements informatiques, les évolutions techniques et fonctionnelles, l'organisation humaine et les responsabilités, la gestion des incidents ou accidents de sûreté.

Cette couverture exhaustive signifie également prendre en compte tous les éléments du Système d'Information qui ont un «besoin de sécurité», c'est à dire dont une atteinte à la sécurité peut avoir un impact sur la réalisation de la mission de la navigation aérienne.

2.1.2 Les mesures de protection doivent être homogènes au sein du Système Informatique. En effet, le niveau de protection effectif du Système Informatique est égal au niveau du plus faible maillon le composant : il est donc vain de vouloir apporter en un point donné des mesures de protection extrêmement lourdes et coûteuses, si par ailleurs en un autre point, aussi sensible, les mesures de protection sont très faibles.

2.1.3 Les mesures de protection doivent être applicables, et donc tenir compte des contraintes et particularités du contexte. Pour cela, dans l'élaboration des règles de sûreté, doivent être considérés : les technologies employées, les contraintes de sûreté de fonctionnement, les habitudes ou usages des exploitants et utilisateurs, etc. Enfin, pour que ces règles soient effectivement appliquées, il est impératif qu'elles soient reconnues par les exploitants et usagers du Système Informatique, qu'ils en aient une bonne connaissance et que ces règles soient applicables au même titre que les règles d'exploitation et d'utilisation déjà existantes par ailleurs.

2.2 C'est en considérant l'ensemble de ces facteurs que la France a lancé une démarche de formalisation d'une politique de sûreté informatique générale et de haut niveau. Ce projet, baptisé «PSINA» (Politique de Sécurité Informatique de la Direction de la Navigation Aérienne) a pour vocation de définir les règles générales de sûreté informatique pour l'ensemble des systèmes «opérationnels» de la navigation aérienne, qui constituent le Système d'Information de Contrôle du Trafic Aérien (SICTA).

Cette politique de sécurité générale doit se traduire par un document, comportant les têtes de chapitre suivantes :

— Objectifs et limites de la PSINA : Définition du Système d'Information pris en compte, principes adoptés, menaces prises en compte, positionnement de la PSINA vis-à-vis d'autres règles existantes par ailleurs;

— Classification des composants du Système d'Information : Quatre niveaux de sensibilité pour les composants fonctionnels et physiques du Système d'Information sont définis ainsi que les critères de classement des composants dans les différents niveaux. La classification s'effectue selon trois axes : la disponibilité, l'intégrité et la confidentialité;

— Accès au Système d'Information par les utilisateurs : Règles d'habilitation, d'accréditation, d'authentification, de traçabilité des actions, règles en cas d'emploi de personnels extérieurs à la Direction Générale de l'Aviation Civile;

— Protection physique : Règles de protection des supports d'information sensibles (médias amovibles, portables...), protection et localisation physique des systèmes informatiques;

— Maintenance et administration du Système d'Information : Règles d'habilitation, d'authentification des personnels de maintenance, règles d'emploi de techniciens de maintenance extérieurs, traçabilité des opérations de maintenance et d'administration des systèmes;

— Interconnexions des systèmes et échanges de données au sein du Système d'Information : Adoption de principes de «zones de confiance» définissant des périmètres de sûreté homogènes, règles d'utilisation de réseaux privés et de réseaux publics pour réaliser des interconnexions internes;

— Interconnexions et échanges de données avec l'extérieur : Règles d'accès au Système d'Information depuis l'extérieur, et règles d'accès du Système d'Information vers l'extérieur, règles d'utilisation de réseaux publics ou de réseaux privés pour réaliser des interconnexions externes, règles concernant l'émission et la réception de données informatiques entre le SI et l'extérieur;

— Évolutions du Système d'Information : Réévaluation de la classification des composants et du niveau de sécurité à chaque évolution du Système d'Information; règles pour l'intégration de nouveaux composants, ou pour le retrait de composants;

— Incidents et accidents de sûreté : Définition d'un incident/accident de sûreté, classification et détection des incidents, actions à mener en cas de détection d'incident de sûreté ; règles de communication interne et externe concernant les incidents et accidents de sûreté; définition des principes de sanctions et poursuites à l'encontre de personnes malveillantes internes et externes à la Direction Générale de l'Aviation Civile;

— Organisation humaine de la sûreté du Système d'Information : Sensibilisation des utilisateurs à la sécurité/sûreté, décisionnaires en matière de sûreté, habilitation des responsables «sûreté», règles d'administration et de maintenance des éléments de sécurisation, etc.

2.3 Afin de s'assurer de l'applicabilité des règles édictées par cette politique de sécurité, et de s'assurer par ailleurs d'une sensibilisation des acteurs du Système d'Information dès l'élaboration de ces règles, un Groupe de Travail a été constitué, et a été chargé de rédiger une proposition de politique. Ce groupe de travail est composé de représentants des différents services opérationnels de la navigation aérienne. Par ailleurs, pour s'assurer que la PSINA pourra effectivement être reconnue comme telle par les différents exploitants et utilisateurs, elle sera approuvée par un Comité d'Encadrement présidé par la Direction de la Navigation Aérienne, lui assurant ainsi une légitimité forte.

2.4 Des exemples de règles de sûreté définies dans le cadre de la PSINA sont présentées ci-dessous :

— Toute interconnexion avec des systèmes externes doit être autorisée formellement par le responsable de sûreté, sur la base d'un dossier de sûreté qui donne notamment les résultats de l'étude de risque qui a été établie en préalable.

— Toutes les interconnexions avec l'extérieur doivent être contrôlées techniquement. Ce contrôle vise notamment à s'assurer, à tout moment, que seuls les services qui ont été autorisés pour cette interconnexion sont accessibles, que seuls les correspondants (utilisateurs ou systèmes) autorisés peuvent l'utiliser, etc. Par ailleurs, le contrôle doit également permettre d'assurer que seuls les services techniques (protocoles réseaux par exemple) strictement nécessaires aux services fonctionnels autorisés peuvent être employés au travers de l'interconnexion.

— Pour les éléments les plus sensibles du Système d'Information, toute interconnexion utilisant des réseaux publics (RTC, Internet...) est interdite.

3. STRATEGIE D'APPLICATION DE LA METHODE ADOPTEE

3.1 Compte tenu de l'ampleur du projet PSINA, et afin de traiter progressivement l'ensemble des aspects, des objectifs prioritaires ont été définis.

Le premier objectif est la maîtrise du périmètre du Système d'Information de la Navigation Aérienne, afin de répondre aux risques d'origine externe. Cette maîtrise du périmètre s'effectue en définissant les fonctions et règles de sûreté qui doivent être appliquées aux frontières du Système d'Information.

Lorsque ce périmètre sera maîtrisé, il sera alors possible de traiter de la sûreté interne. La réponse aux risques internes est beaucoup plus difficile à définir et les moyens à mettre en place plus importants car il n'est pas possible de tout «verrouiller» : le Système d'Information doit en effet rester utilisable et performant, et il n'est donc pas possible d'adopter des mesures de protection aussi radicales et relativement simples que celles employées vis-à-vis de l'extérieur. C'est l'une des raisons principales pour laquelle il a été choisi de traiter cet aspect en second lieu.

3.2 Au travers de ce séquencement des objectifs à atteindre, l'objectif final est de parvenir à mettre en place une sûreté en «profondeur» du Système d'Information, consistant en une défense périmétrique, constituée techniquement par des dispositifs de contrôle et de sûreté agissant au niveau des réseaux et interconnexions de réseaux, et une défense interne, constituée techniquement par des dispositifs de sûreté se positionnant au niveau du réseau interne et des systèmes eux-mêmes.

4. CONCLUSION

4.1 La France poursuit actuellement les travaux de définition d'une première version de sa politique de sécurité informatique. Une proposition de rédaction des premiers chapitres constituant le socle de cette politique (objectifs, limites de la politique et règles de classification des composants du Système d'Information) a d'ores et déjà été élaborée par le Groupe de Travail, qui poursuit actuellement ses travaux concernant les règles d'interconnexion avec l'extérieur. Cette première proposition sera bientôt présentée au Comité d'Encadrement.

4.2 Lorsque ces premiers chapitres auront été complétés par celui concernant l'organisation humaine de la sécurité informatique, une première version de la Politique de Sécurité Informatique de la Navigation Aérienne pourra être officiellement mise en œuvre au sein de la navigation aérienne française.

4.3 Ce travail, de longue haleine, devra ensuite être poursuivi, afin d'aboutir à une politique de sécurité complète et conforme à ses objectifs.

5. ACTION PAR LA CONFERENCE

5.1 La conférence est invitée à :

a) prendre en considération les risques qui menacent les systèmes informatiques de la navigation aérienne;

b) élaborer des SARPS en matière de sécurisation des systèmes informatiques;

c) charger un groupe d'experts de réaliser un guide général visant à aider les Etats à mettre en œuvre leur politique de sécurité et de sûreté, par exemple sous la forme d'une «check list» indiquant les points et questions devant être traités dans une politique de sécurité et de sûreté ainsi que les moyens de sécurisation des systèmes informatiques.

— FIN —