La SSI : une nouvelle mission !

Tout utilisateur se doit d'obéir à des consignes précises découlant du règlement interne édicté par son employeur. Et il en est de même dès que l'utilisateur sera averti d'une attaque informatique.

Un superviseur est bien un utilisateur comme un autre : il utilise un ensemble d'outils de gestion, appelés « supervisions techniques spécialisées » (STS), lui permettant de gérer en temps réel la disponibilité opérationnelle des chaînes techniques dont il a la charge.

Ainsi que les responsables d'exploitation, les administrateurs système et les gestionnaires de réseau qui ne sont que des utilisateurs particuliers au regard de la sécurité des systèmes d'information : s'ils peuvent être responsables du bon fonctionnement du réseau ou des systèmes qui y sont connectés, ils ne sont pas nécessairement compétents dans le domaine de la SSI.

Seuls les correspondants de sécurité (autrement dit les ASSI) ont une compétence reconnue dans le domaine de la SSI.

L'entité en mesure d'évaluer les menaces est le « comité de sécurité des réseaux » (aujourd'hui plus fréquemment désigné par l'abréviation CSIRT). Ce comité est composé des correspondants de sécurité locaux, des représentants des autorités hiérarchiques concernées et de spécialistes dans le domaine des réseaux : Ils sont les « experts en sécurité des systèmes d'information ». Ils peuvent par exemple donner des avis et des directives aux utilisateurs face aux menaces.

Cette compétence particulière s'articule autour de 3 grands domaines :

- la sécurité informatique dans tous ses composants ;
- la protection des communications ;
- la protection contre les signaux compromettants.

Le référentiel métier du titre ESSI, délivré par le Centre de Formation à la Sécurité des Systèmes d'Information, donne une idée plus précise des compétences associées.

En aucun cas il ne peut s'agir d'une fonction assimilable à de la « supervision technique » ou à de la « maintenance ». La fonction SSI constitue un domaine bien distinct.

Les IESSA du CESNAC n'accepteront pas d'être des experts SSI au rabais. Si nous sommes parfaitement conscients de la nécessité d'afficher une réponse aux enjeux de sécurité-sûreté actuels, nous ne cautionnerons pas une énième démarche bricolée nous privant des moyens indespensables pour rendre un service décent.

La clé permettant d'engager une démarche professionnelle est la prise en compte de cette nouvelle mission dans notre statut (conformément au mandat donné par le directeur des services de la navigation aérienne dans le cadre du groupe de travail national CESNAC).

Nous demandons que la « mission de sécurité des systèmes d'information opérationnels » soit intégrée dans le statut des IESSA.

Les IESSA du CESNAC réunis en intersyndicale

Modification (ajout) de l'article 2 du décret n° 91-56 du 16 janvier 1991 portant statut du corps des ingénieurs électroniciens des systèmes de la sécurité aérienne

Les ingénieurs électroniciens des systèmes de la sécurité aérienne sont chargés, dans les organismes de la navigation aérienne, d'assurer la maintenance et la supervision technique des équipements et des systèmes qui contribuent à la sécurité des vols, de participer au développement de ces équipements et systèmes et d'exécuter, dans l'administration de l'aviation civile, des missions **de sécurité des systèmes d'information opérationnels,** d'encadrement, d'instruction, d'étude, de recherche ou de direction de service ou de partie de service.

REFERENTIEL METIER « Expert SSI »

d'après l'agence nationale de la sécurité des systèmes d'information

L'Expert en sécurité des systèmes d'information doit garantir la sécurité des systèmes d'information tout au long de leur cycle de vie, en intervenant aux différentes étapes, depuis l'expression de besoin jusqu'à l'exploitation, en passant par le développement.

Compétences	Objectifs
Connaître et formaliser les besoins de sécurité	Être conscient des enjeux de la sécurité et prendre en compte toutes les dimensions (technique, organisationnelle, humaine, juridique, réglementaire) de la problématique SSI.
	Être capable de mener, de manière formelle, l'analyse d'un projet relatif à un système d'information complexe afin d'identifier les besoins en sécurité, les menaces et les risques, et d'en déduire les objectifs de sécurité.
	Être capable de conseiller ou de convaincre un donneur d'ordre (autorité, chef de projet, chef DSI…) dans le domaine de la SSI.
Élaborer un dispositif technique correspondant aux besoins de sécurité	Comprendre les problématiques de sécurité, notamment connaître et savoir identifier les risques liés à un système d'information (par domaine ou de manière globale).
	Comprendre les forces et faiblesses des produits de sécurité, notamment ceux mettant en œuvre des mécanismes cryptographiques.
	Être capable de définir une solution technique pour défendre un système d'information selon les grands axes de la défense en profondeur.
	Être capable de faire des recommandations relatives à la SSI auprès d'un spécialiste technique d'un système d'information.
Savoir estimer ou faire estimer le niveau de sécurité d'un dispositif	Estimer soi-même le niveau de sécurité d'un système d'information.
	Connaître les différentes modalités d'un audit et savoir le préparer.
	Savoir prendre en compte les résultats d'un audit, élaborer et conduire un plan d'action.
	Savoir établir une démarche d'homologation et bien la conduire.
Gérer la sécurité d'un système d'information	Être un interlocuteur auprès des acteurs du projet, des spécialistes informatiques, des administrateurs et des RSSI.
	Maintenir le niveau de sécurité du système d'information, adapté aux contraintes métier.
	Savoir formaliser les documents SSI.
	Savoir veiller sur les dernières vulnérabilités, menaces et produits de sécurité et savoir les analyser.
	Évaluer les impacts d'une vulnérabilité ou d'une menace.
	Savoir détecter et gérer un incident de sécurité.