

Utilisation du fichier analyse de risque générique « Périmètre administratif »

(5/10/09)

Le but de ce fichier est d'être utilisable par l'ensemble des unités CNRS/UPMC pour faire une analyse de risque des données du périmètre administratif. Nous avons essayé d'être à la fois générique et précis, en éliminant de base tout ce qui nous paraissait non adapté à nos laboratoires.

1. Rappel de définitions

Les **Actifs primordiaux** représentent les données ayant **une importance pour l'unité**. Cette notion d'importance est à garder à l'esprit pour ne pas sombrer dans une exhaustivité fatale.

Les **actifs de soutien** représentent les supports informatiques qui hébergent les actifs primordiaux.

Les **Menaces** représentent tout ce qui peut attaquer les actifs primordiaux

Les **Vulnérabilités** représentent les propriétés intrinsèques d'un actif primordial qui l'expose à des menaces

Le **Risque** représente la possibilité qu'une menace exploite une vulnérabilité d'un actif primordial pour lui porter préjudice.

Exemples :

- **Risque** qu'une base de données (**actif primordial**), hébergée sur un ordinateur portable (**actif de soutien**) voit ses données détruites parce que l'ordinateur peut être facilement volé (**menace**) car il est portable (**vulnérabilité**).
- **Risque** que les données liées aux commandes de l'unité (**actif primordial**) soient divulguées car un utilisateur mal intentionné veut se venger (**menace**) de l'unité or les données financières sont sur un serveur (**actif de soutien**) accessible à tous (**vulnérabilité**).

2. Principes généraux du fichier

Les données (actifs primordiaux) ont été regroupées en types liés à des applications connues du Système d'Information du CNRS et de l'UPMC. Certaines unités peuvent avoir d'autres tutelles et/ou avoir développé leurs propres applications S.I, il faudra penser à les rajouter dans le classement par types.

Les applications et leurs actifs primordiaux sont dans le classeur « applis nationales et locales »

Chaque type de données (et ses applications) est analysé dans un onglet spécifique : par exemple, les données de type Ressources Humaines sont analysées dans l'onglet « RH ».

On s'aperçoit que pour des applications nationales (ce qui est très souvent le cas) les données (actifs primordiaux) à prendre en compte sont souvent **des copies ou des extractions** dans l'unité des données de l'application. En clair l'application nationale n'est pas dans le périmètre de PSSI de l'unité, dans ce cas seul le critère de confidentialité des données doit être retenu pour l'unité.

Nous avons essayé de mettre beaucoup de champs sous forme de listes déroulantes pour une adaptation la plus simple possible.

3. Processus :

- Chaque type de données est **valorisé** (en terme de confidentialité, d'intégrité et de disponibilité) d'une façon générique que les laboratoires pourront adapter à leur cas.
- Nous avons listé **toutes les menaces** qui nous paraissaient possibles/réalistes dans le contexte de nos unités. Cette liste a été faite **au regard des critères de sensibilité choisis**. Par exemple si seul le critère de confidentialité est retenu il est inutile de regarder les menaces concernant la disponibilité ou l'intégrité. Les laboratoires pourront/devront revoir ces critères et cette liste en fonction de leurs spécificités. Pour chaque menace listée il faut imaginer et renseigner l'**impact** possible. Cela permettra un **suivi** de l'analyse de risque (savoir 1 an après pourquoi ce choix a été fait n'est pas toujours facile...). Si une menace n'est pas retenue on ne regarde même pas les vulnérabilités mais il est intéressant de se rappeler qu'on a choisi de ne pas retenir une menace...
- Pour chaque menace plausible nous avons listé **les vulnérabilités** qui nous semblaient réalistes. Là aussi nous n'avons pas retenu toutes les vulnérabilités mais uniquement celles qui nous ont semblées probables **compte tenu des critères de sensibilité**.
- Pour chaque vulnérabilité le laboratoire doit calculer le risque associé en renseignant **la vraisemblance** et **la facilité de mise en œuvre** qui sont évidemment très dépendants de l'unité et donc qui n'ont pas été renseignés. Le risque est calculé automatiquement suivant l'abaque décrit dans l'onglet « Abaque ».
- Pour chaque vulnérabilité nous avons précisé **les objectifs de sécurité** à atteindre. Ces objectifs correspondent aux futurs chapitres de la PSSI de l'unité décrivant la politique de sécurité. Nous avons essayé de détailler **les mesures de sécurité** qui correspondent à ces objectifs mais c'est typiquement ce que les laboratoires devront préciser et détailler. Même si une mesure existe déjà il faut la lister. Nous avons choisi de ne faire figurer que 3 mesures au maximum.
- Les mesures décrites sont formulées en **utilisant la norme ISO** qui n'est pas forcément très très lisible... Il faudra donc, dans le document final de PSSI (qui comprendra un chapitre par objectif et un paragraphe par mesure), reformuler simplement d'une façon compréhensible par tous, sans rentrer dans les aspects techniques, les mesures préconisées.