CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

Modèles et fonctions de calcul

Évaluation et simulation : de la théorie à la pratique

Des fonctions de calcul nécessaires

Le modèle de risque impose un minimum de fonctions de calcul pour estimer les niveaux de risque :

- Niveaux de qualité des services de sécurité
- Facteurs de réduction de risques
- Effets combinés de plusieurs services et de plusieurs facteurs
- Estimation des paramètres du risque
- Estimation de la gravité du risque

Une confiance raisonnée

Les mécanismes de calcul peuvent donner une fausse impression de précision :

- Certains paramètres, nécessaires pour les calculs, sont des estimations et non des mesures scientifiques
- Les formules elles-mêmes sont raisonnables et rationnelles mais ne sont pas « démontrables »

Il reste que, comme tout processus d'analyse, les modèles de calcul permettent de décomposer un problème complexe en problèmes élémentaires plus simples.

Ce sont des supports au raisonnement et des aides à la décision

Une confiance raisonnée

L'absence de modèle de calcul n'est en rien une solution :

- Mieux vaut des modèles de calcul que l'on sait devoir contrôler et maîtriser que pas de modèles du tout.
- Le problème, si problème il y a, est dans la pratique et l'usage de ces modèles.

La confiance dans les modèles repose également sur un principe de prudence adopté lors de la construction des bases de connaissance

Une confiance raisonnée

La construction de la base de connaissance du CLUSIF a été menées avec un tel principe de prudence :

- Prise en compte de la robustesse et de la mise sous contrôle (ou permanence) dans l'évaluation de la qualité d'un service de sécurité.
- Prise en compte des services de sécurité si et seulement si on peut garantir qu'ils auront une effet.
- Prudence dans les grilles de décision

La mise en pratique

Les automatismes de calcul restent des aides essentielles, si ce n'est indispensables, pour :

- Faire une présélection de plans d'action susceptibles de réduire les risques
- Mettre en évidence les risques non réduits par les actions décidées
- Simuler l'effet des mesures décidées sur les niveaux de risques résiduels
- Piloter la sécurité de l'information par la gestion des risques

La mise en pratique

Une mise en pratique raisonnée consiste alors à définir et sélectionner des projets à déployer en fonction des présélections présentées par les automatismes mais aussi de l'expérience des acteurs (RSSI en particulier)

Un usage recommandé des automatismes est alors de simuler l'effet des projets de sécurité envisagés sur l'ensemble des situations de risque pour mettre en évidence les risques non réduits (ou insuffisamment réduits et restant inadmissibles)

La mise en pratique

Un contrôle hors automatismes, basé sur le modèle général des risques, tant des risques les plus graves que des risques non réduits, est toujours recommandé

La mise en pratique

Méhari 2010 incorpore différentes fonctions de calcul :

- Ce sont des aides essentielles dans les processus de décision
- Ce ne sont que des aides à la décision

Merci de votre attention