Chapitre 1 - Intérêts des méthodes quantitatives d'analyse des risques

Les méthodes quantitatives et qualitatives d'évaluations ne sont opposées, chacune d'elles à ces avantages et ses propres limites. En approche quantitative, nous utiliserons des méthodes statistiques, nous utiliserons des données chiffrées et nos enquêtes seront plus structurées avec des questions plutôt fermées. On procédera à des mesures avec un échantillon plus vaste que dans le cas de recherche qualitatives. à chaque étape du processus Correspondent des outils méthodologiques (récolte des données, analyse, réajustement).

On caractérise quelque fois les méthodes en les classant en 3 catégories :

La méthode quantitative : elle implique de prendre un nombre important de mesures pour calculer le coût des dommages, idéalement en termes financiers, et les effets des mesures de réduction prises. Cette analyse quantitative de risque nécessite de s'appuyer sur des faits et des chiffres avérés et constitue souvent un exercice long et délicat qui n'est pas approprié aux risques des systèmes d'information.

La méthode qualitative : elle fournit une voie plus facile pour mesurer la valeur des actifs et les probabilités de menaces. Ces valeurs peuvent être décrites en utilisant des expressions simples telles que "haut", "moyen" et "faible". Cette approche corrige les imperfections de l'approche quantitative en réduisant l'incertitude inhérente aux chiffres.

L'approche par base de connaissance : elle implique de réutiliser les bonnes pratiques en matière de connaissance des risques d'organismes semblables (en taille, périmètre et/ou marché). En complément de la méthode qualitative, elle permet d'aller vite pour des risques «courants». La méthode quantitative semble beaucoup plus sérieuse puisque elle s'appuie sur des données chiffrées en termes de probabilité (fréquence). Malheureusement, il existe très peu de données corrélées sur la sinistralité informatique. Dans l'industrie, il existe des approches de type SIL SIS permettant, en s'appuyant sur des logiciels et des bases de données de quantifier les niveaux de risques.