Le management des risques avec

MEHARI

Méthode développée et supportée par le CLUSIF

Novembre 2007

Sommaire

Contenu du management des risques

Méhari fournit un cadre méthodologique, des guides et des bases de connaissance pour pouvoir répondre aux questions suivantes :

- **Quels sont les situations de risque auxquelles l'entreprise ou l'organisation est confrontée ?**
- **Quel est le niveau de risque correspondant actuellement à chaque situation identifiée ?**
- **Chacune de ces situations est-elle acceptable ?**
- **Que peut-on faire pour réduire chaque risque critique ?**
- **Quels outils utiliser pour suivre régulièrement l'état des risques**

Sommaire

L'identification des situations de risque

Dans Méhari, une situation de risque est décrite par :

- **Un élément d'actif qui est en situation de risque**
  - **tel que : information, données applicatives, documents écrits, élément de réseau, serveur, etc…**
- **Un type de dégradation subie par cet élément**
  - **Perte de disponibilité, d'intégrité, de confidentialité, etc…**
- **Les circonstances pouvant conduire à cette dégradation**
  - **Événement naturel, détournement volontaire de fichier, panne matérielle, effacement de données par virus, etc…**

L'identification des situations de risque

L'actif qui est en situation de risque peut être :

- **Un élément particulier :**
  - Serveur de la Direction financière
  - Données relatives au personnel
  - Fichier de configuration des réseaux
  - etc…
- **Un groupe homogène d'actifs de même nature :**
  - Ensemble des serveurs de données bureautiques
  - Données applicatives
  - Les locaux informatiques
  - etc.

L'identification des situations de risque

Les circonstances pouvant conduire au risque décrivent :

- **Le type générique de menace :**
  - **Détournement de données**
  - **Perte de fichiers**
  - **etc…**
- **Le mode d'action ou de réalisation de cette menace :**
  - **Copie après usurpation d'identité**
  - **Vol de support**
  - **Effacement après acquisition illicite de droits**
  - **etc.**
- **Éventuellement l'acteur mettant à exécution la menace :**
  - **Utilisateur**
  - **Hacker**
  - **Personnel**

L'identification des situations de risque

Dans Méhari, les vulnérabilités exploitées ne font pas partie de la description des risques :

- **Les vulnérabilités évoluent, avec le temps et avec l'architecture, et une vulnérabilité faible aujourd'hui peut se révéler forte demain**
- **La multiplicité des vulnérabilités potentielles pour certaines situations de risque compliquerait leur description et/ou multiplierait inutilement le nombre de risques à traiter**
- **Les vulnérabilités seront mieux prises en compte lors de l'évaluation des risques et lors de leur réduction**

L'identification des situations de risque

Les situations de risque couramment rencontrées sont décrites dans les bases de connaissances de Méhari :

- **Plus de 180 « scénarios de risque » dans Méhari-2007**
- **Chaque situation de risque est décrite dans un manuel de référence des scénarios de risque**

Des situations de risque spécifiques peuvent être décrites, si nécessaire, en complément

L'identification des situations de risque

Exemples de situations de risque issues des bases de connaissances de Méhari :

- **Panne rendant indisponible un équipement de réseau**
- **Arrêt d'une application critique dû à un bug logiciel**
- **Petit vandalisme sur des systèmes centraux, par des personnes autorisées à pénétrer dans l'établissement**
- **Modification volontaire des fonctionnalités prévues d'une application, par les équipes de développement**
- **Accès au système et consultation en ligne de données sensibles par un membre du personnel autorisé de manière illégitime**

Sommaire

L'analyse des risques

Dans Méhari, l'analyse de risque est une évaluation quantitative du niveau de gravité de chaque situation de risque, résultant de :

- **La valeur de l'élément d'actif concerné (sa classification), pour le type de dégradation envisagé**
- **La probabilité de survenance de l'événement à l'origine du risque**
- **La qualité des services de sécurité pouvant avoir un effet de réduction du risque**

L'analyse des risques

La valeur des éléments d'actif, pour chaque type de dégradation envisagé, est évaluée par un module spécifique :

- **Processus : Analyse des enjeux et classification**
- **Supports : Guide spécifique, tableaux standards à remplir, exemples**
- **Livrables : Échelle de valeurs des dysfonctionnements et tableaux de classification des éléments d'actifs**

L'analyse des risques

La probabilité de survenance de l'événement à l'origine du risque est évaluée lors d'une étape spécifique de la méthode :

- **Processus : Analyse des expositions aux risques**
- **Support : Guide d'analyse, tableau standard à évaluer, valider ou modifier**
- **Livrables : Tableau des « expositions naturelles » aux causes de risque**

L'analyse des risques

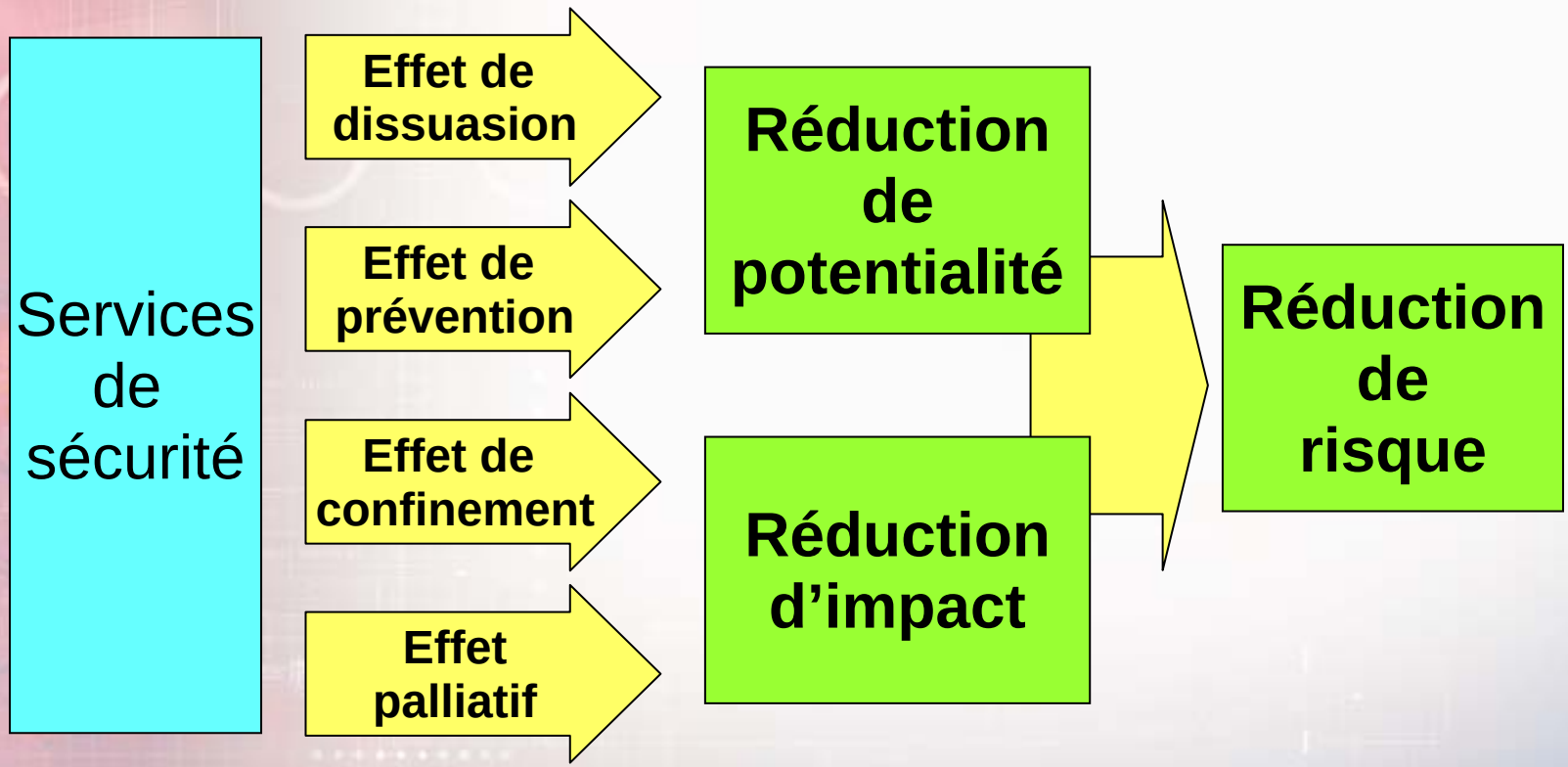
Pour une situation de risque donnée, certains services de sécurité peuvent avoir un effet de réduction du risque

Cet effet est plus ou moins important, selon la qualité des services de sécurité :

- **La qualité des services est mesurable par un audit**
- **Des questionnaires d'audit sont inclus dans les bases de connaissances de Méhari**
- **Une méthode et des mécanismes d'évaluation de la qualité des services de sécurité sont également inclus**

L'analyse des risques

Les effets des services de sécurité peuvent être de différentes natures



L'analyse des risques

L'effet de réduction du risque des services de sécurité est évalué lors d'une étape spécifique:

- **Les services pertinents, ainsi que leurs effets sur chaque situation de risque, sont indiqués et commentés dans la base de connaissances Méhari**
- **Les effets de réduction de risque de ces services sont quantifiables, en fonction de leur qualité**
- **L'ensemble des méthodes et outils d'évaluation de la réduction de risque sont décrits dans Méhari**

L'analyse des risques

La quantification des éléments caractéristiques du risque :

- **valeur d'actif,**
- **probabilité d'occurrence**
- **facteurs de réduction de risque**

permettent de faire une évaluation quantitative de la gravité de chaque risque

L'analyse des risques

Le processus d'analyse des risques comprend :

- L'analyse des enjeux et la classification (valeurs d'actifs)
- L'analyse des menaces et de leur probabilité d'occurrence
- L'audit des services de sécurité
- L'évaluation des facteurs de réduction de risque
- Le contrôle et la validation des éléments précédents
- L'évaluation de la gravité de chaque situation de risque
- Un jugement sur le caractère acceptable ou non de chaque situation de risque

L'analyse des risques

Le processus d'analyse des risques s'appuie sur :

- Un guide d'analyse de risque
- Les questionnaires d'audit de la base de connaissances
- Des manuels de référence (services de sécurité et scénarios de risque)

Les livrables comprennent :

- La liste de risques avec une évaluation individuelle de leur gravité
- La liste des risques critiques

L'analyse des risques

Points clés de l'analyse des risques :

- Évaluation des enjeux (conséquences) par les responsables d'activités :
  - Gravité réelle des conséquences plutôt que niveau de gêne ressentie par les utilisateurs
- Évaluation des probabilités a priori par les professionnels de la sécurité
- Évaluation de l'effet des mesures de sécurité :
  - audit détaillé
  - Prise en compte de multiples effets de réduction de risque

Sommaire

La réduction des risques critiques

Dans Méhari, la réduction des risques critiques est concrétisée par une ensemble de décisions prises pour que chaque situation de risque critique soit ramenée à un niveau acceptable

Ces décisions couvrent :

- **Les services de sécurité à améliorer**
- **Le niveau objectif pour la qualité de chaque service**

Nota : ceci n'est possible que grâce au modèle d'évaluation quantitative du risque offert par Méhari

La réduction des risques critiques

Pour chaque situation de risque critique, les bases de connaissances de Méhari permettent :

- **L'identification des services de sécurité ayant un effet sur le niveau de gravité du risque**
- **La mesure de l'effet des améliorations possibles de services de sécurité sur la gravité du risque et donc une sélection optimisée des mesures à prendre**
- **La simulation de l'état des risques résiduels en fonction des actions d'amélioration envisagées**

La réduction des risques critiques

Il est ainsi possible d'établir des plans d'amélioration des services de sécurité propres à rendre acceptables tous les risques critiques :

- **Soit en travaillant risque par risque**
- **Soit en utilisant un module d'optimisation permettant de s'attaquer en priorité aux services de sécurité dont l'amélioration aura le plus d'effet**

Sommaire

Le pilotage du management des risques

Les plans d'amélioration des services de sécurité peuvent être regroupés en projets :

- Regroupant des ensembles homogènes de services de sécurité à améliorer, par exemple :
  - Projet « Plans de secours » : Sauvegardes, Plans de reprise d'activité, Plans de continuité métiers, …
  - Projet « Protection des données applicatives » : Gestion des habilitations, Authentification, Gestion des accès, …
- Avec des dates de début et d'achèvement par projet
- Fixant des objectifs de qualité par service de sécurité

Le pilotage du management des risques

Il est ainsi possible de mettre en place des tableaux de bord indiquant :

- **Le nombre de situations de risque par niveau de gravité**
- **Le nombre de risques critiques en fonction du temps**

et de mettre à jours ces tableaux de bord en fonction d'audits périodiques de sécurité

Sommaire

La documentation et les supports de MEHARI

La documentation de Méhari comprend :

- Une présentation générale de la méthode (français, anglais, allemand, espagnol, italien)
- Une guide de présentation des principes et mécanismes (français et anglais)
- Un guide de l'analyse des enjeux et de la classification (français et anglais)
- Un guide du diagnostic des services de sécurité (français et anglais)
- Un guide de l'analyse des risques (français et anglais)

La documentation et les supports de MEHARI

La documentation de Méhari comprend :

- **Un manuel de référence des services de sécurité :**
  - une fiche par service décrivant les objectifs, les mécanismes mis en œuvre et les critères de qualité du service
- **Un manuel de référence des scénarios de risque de la base de connaissance :**
  - une fiche par scénario décrivant le contexte et les facteurs influant sur les divers paramètres de risque

La documentation et les supports de MEHARI

Les « bases de connaissances »,

livrées sous forme de fichiers Excel (français et anglais)

- **Constituent une base puissante pour manager la sécurité de l'information**
- **Établissent des liens entre :**
  - les enjeux
  - les ressources du SI
  - les menaces et les parades
- **Contiennent les formules utilisées pour le calcul de :**
  - la qualité des services de sécurité audités
  - la gravité des scénarios de risque

La documentation et les supports de MEHARI

L'ensemble de la documentation et des bases de connaissances de Méhari est disponible en libre téléchargement sur le site du CLUSIF :

www.clusif.asso.fr

La documentation et les supports de MEHARI

MEHARI est supporté par un outil du marché maintenu en conformité avec les évolutions ou variantes des bases de connaissances :

RISICARE™ de Buc SA.

Questions ?