ONSERVATOIRE NATIONAL DES ARTS ET METIERS
PARIS

PROBATOIRE

présenté en vue d'obtenir

le DIPLOME D'INGENIEUR C.N.A.M.

en

INFORMATIQUE RESEAUX SYSTEME MULTIMEDIA

par

Didier BALLOY

Le *RISQUE INFORMATIQUE* Comment y remédier ?

Soutenu le 21 janvier 2002

JURY

PRESIDENT : M. Jean-Pierre ARNAUD

Remerciements

Je remercie

Mme Annie DUPONT, membre du CLUSIF[1], de m'avoir présenté les objectifs de cet organisme et de m'avoir fourni un explicatif de la méthode MEHARI, méthode issue du club et des concepts gravitant autour de cette méthode d'analyse.

M. Daniel TABET, membre de l'ISDF[2] de m'avoir expliqué les concepts fondamentaux de la sûreté de fonctionnement et développement du logiciel.

Mme Nathalie CAO et M. Jean-Jacques CHANDEZ pour leur aide et compétence en matière de recherche bibliographique et de m'avoir guidé dans l'élaboration de mon mémoire de probatoire.

A l'issue de ces différents contacts, ces personnes m'ont permis d'accéder à des organismes qui m'étaient inconnus jusqu'à présent, élargir mes contacts techniques auprès de spécialistes de la sécurité et de la sûreté de fonctionnement, mais aussi de découvrir l'importance et la place que doit prendre l'analyse des risques informatiques dans un projet, voire dans toute entreprise.

[1] CLUSIF : *Club de la Sécurité des Systèmes d'Information Français*
[2] ISDF : *Institut de la Sûreté De Fonctionnement*

Table des matières

1 Introduction

Selon une définition du dictionnaire[3], le risque est un « *danger, inconvénient plus ou moins probable auquel on est exposé* ». L'objet de ce document est de traiter le risque informatique et les solutions pour y remédier.

Nous verrons dans le premier chapitre qu'il existe plusieurs formes de risques - dont nous détaillerons la typologie - ainsi que leurs conséquences surtout si aucun traitement n'est appliqué. Nous aborderons la problématique du risque informatique au travers de ses concepts et des principales méthodes permettant de les analyser et les moyens pour les anticiper.

Pour pouvoir se protéger des risques, il convient d'en définir les origines possibles : organisation, documentation, milieu, environnement du système d'information et interventions humaines sont autant de facteurs clairement identifiés. Nous aborderons l'analyse, l'évaluation et les méthodes de modélisation des risques afin de les maîtriser ou du moins les réduire.
Un chapitre est donc consacré aux remèdes possibles avec différentes techniques permettant d'améliorer la disponibilité d'un système d'information et de minimiser sa vulnérabilité par le biais d'outils et de modélisations.

La sécurité dans les systèmes d'information et les réseaux nécessite que nous y attachions une grande attention au sein des entreprises, afin d'éviter les éventuelles vulnérabilités. Nous le verrons dans le chapitre *Techniques d'amélioration de la sécurité*. Notre sujet sera clôturé en abordant des méthodes de reprises d'activité suite à l'interruption d'un service et à l'apparition éventuelle d'un sinistre.

L'objectif de ce document est de tenter de mettre en évidence les concepts régissant le risque informatique, passer en revue des techniques palliatives via des outils ou des méthodes afin de prévenir ou remédier à un sinistre prévisible ou non.

2 Risque informatique

Dans ce chapitre, nous allons dans un premier temps aborder différentes *définitions* du risque, les *typologies* de risque les plus connues, certaines *conséquences* dues à l'apparition d'un événement, et quelques *moyens de lutte* contre les risques les plus fréquemment mis en œuvre dans les entreprises.

Ensuite, les notions de *sécurité*, *vulnérabilité* ainsi que leurs *causes et effets* seront étudiées, immédiatement suivies par la présentation de certains *outils* permettant la *modélisation* d'un risque.

Nous présenterons ensuite plusieurs *exemples* de risques nous permettant de définir les différents *types* en fonction de la *classification* de l'Assemblée Plénière des Sociétés d'Assurances Dommages (APSAD).

Nous verrons enfin *les méthodes de mesure des risques* permettant d'apprécier un risque et d'amener une solution pour pallier un sinistre éventuel.

[3] 🕮 Source : Dictionnaire *Larousse.*

2.1 Définition

Le risque est un *événement contingent et dommageable* pouvant entraîner des modifications partielles voire neutraliser totalement un système d'information.

En sécurité informatique, le risque est lié à l'éventualité d'une menace informatique volontaire ou involontaire, interne ou externe au système d'information.
Le risque informatique est lié à la connaissance du métier, au niveau de maîtrise de l'outil informatique ainsi qu'à l'utilisation des moyens de contrôles (tests unitaires, tests par lots, recettes, contrôles, audits des privilèges informatiques, etc).
D'autre part, le risque informatique dans une entreprise est étroitement lié à la dépendance de cette entreprise par rapport à son système d'information.

2.2 Typologie

Selon l'APSAD, la typologie des risques regroupe trois catégories principales, elles-mêmes décomposées en sous-catégories selon la nature du risque.
Ci-dessous des tableaux récapitulant les risques (accidents, erreurs, malveillances) et leur types (A1 à A4, E1 à E2, M1 à M6) recensés par l'APSAD.

		ACCIDENTS
A1	*Pannes*	Matérielles et logiques
A2	*Evénements naturels*	Inondation, tempête, cyclone, vent, ouragan, foudre, grêle, neige (poids sur les toitures), phénomène sismiques et volcaniques, etc.
A3	*Perte de services essentiels*	Electricité, télécommunication, eau, fournitures spécifiques, fluides.
A4	*Autres risques accidentels*	Chocs, collisions, chutes, introduction de corps étrangers solides, liquides, gazeux ou mixtes phénomènes ayant des actions physiques ou chimiques, pollution par rayonnement

Figure 1 - Typologies des accidents

		ERREURS
E1	*Erreurs d'utilisations*	Erreurs de saisie, de transmission d'exploitation du système
E2	*Autres erreurs*	Erreurs de conception et de réalisation logicielles

Figure 2 - Typologies des erreurs

		MALVEILLANCES
M1	*Vol*	Matériels principaux ou accessoires, vandalisme sur le matériel
M2	*Fraude*	(cf. lexique)
M3	*Sabotage*	attentat, vandalisme, action malveillante conduisant à un sinistre matériel
M4	*Attaques logiques*	Bombes logiques, parasites, Cheval de Troie, sniffer, spoof virus, ver (cf. lexique)
M5	*Divulgation*	(cf. lexique)
M6	*Autres*	Grèves, contrefaçon du logiciel, pertes ou indisponibilité de personnel

Figure 3 - Typologies des malveillances

Ces listes ne sont pas exhaustives et sont susceptibles d'être modifiées en fonction de l'évolution des différentes atteintes du système d'information.

Conséquences

Les conséquences de ces risques ont un impact sur les coûts financiers de l'entreprise voire même sur le matériel lui-même.
De ce fait, nous distinguerons plusieurs types de conséquences – directes (ayant un impact sur le matériel et non-matériel) et indirectes (engendrant une dépense financière : frais supplémentaires, pertes de fonds et de biens, etc) - pouvant être classifiés de la façon suivante :

	CONSEQUENCES DIRECTES
Matériel	• Frais d'expertises • Frais de réparation du matériel • Frais de remplacement éventuel du matériel
Non-matériel	• Frais d'expertises • Frais de restauration du système d'exploitation • Frais de restauration des données • Frais de restauration des programmes • Frais de restauration des procédures • Frais de restauration des documentations

Figure 4 - Conséquences directes

	CONSEQUENCES INDIRECTES
Frais supplémentaires	• Pertes d'exploitation
Perte de fonds et de biens	• Pertes de biens physiques • Pertes d'informations confidentielles, de savoir-faire • Pertes d'éléments non reconstituables du système
Autres pertes	• Utilisation non autorisée de ressources • Copie illicite • Pertes qualitatives => image de marque dégradée, pertes de compétitivité

Figure 5 - Conséquences indirectes

2.3 Moyens de lutte

A titre indicatif, voici la répartition des moyens mis en œuvre par les entreprises pour lutter contre le risque informatique sur l'année 2000, ressortant d'une étude de l'APSAD[4], sur un échantillon de 433 entreprises réparties en 3 classes :

- *10 à 199 employés*
- 200 à 499 *employés*
- supérieur à 500 *employés*

Sur cet échantillon, seuls 5 secteurs d'activités sont intégrés :

1. *industries*
2. *services*
3. *transports et télécom*
4. *commerces*
5. *bâtiments et travaux public*

[4] APSAD : *Assemblée Plénière des Sociétés d'Assurances Dommages*

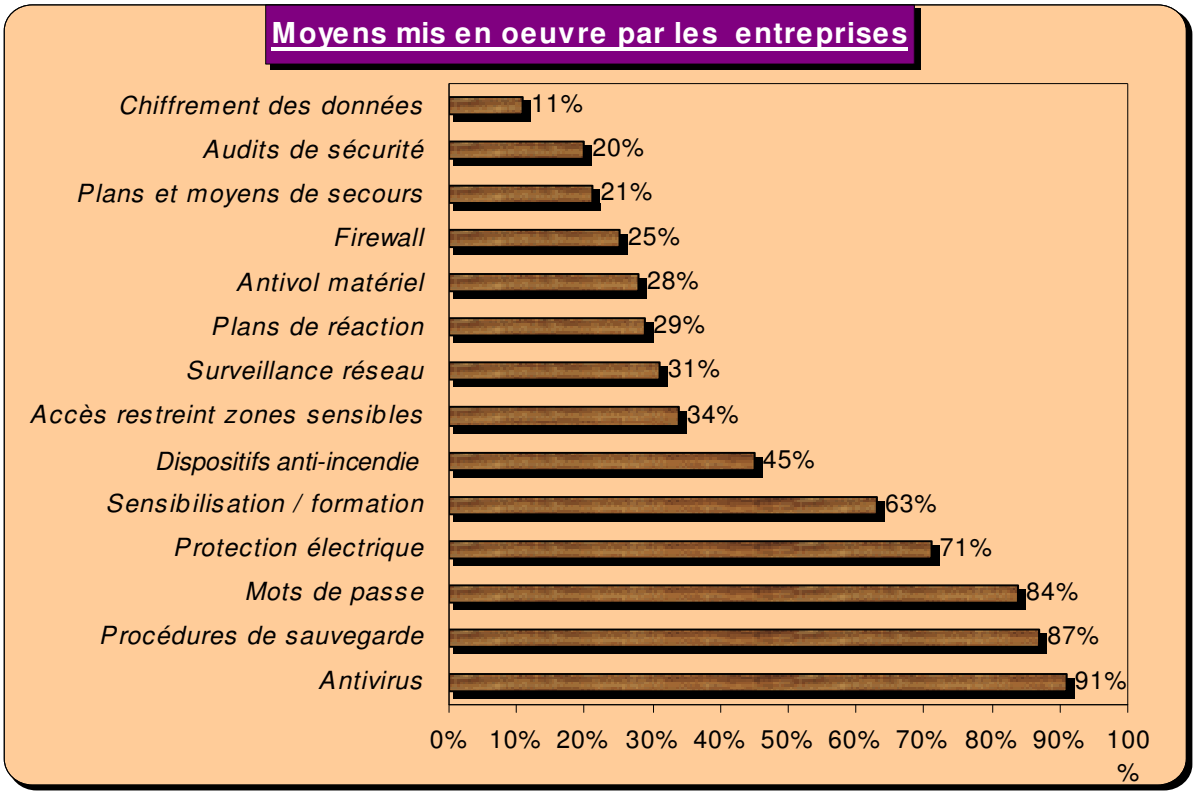


Figure 6 - Moyens de lutte mis en œuvre par les entreprises (étude APSAD)

2.4 Sécurité, vulnérabilité, causes, effets

La sécurité est la non-occurrence de défaillance catastrophique et la prévention d'accès et/ou de manipulations non autorisés de l'information[5].

2.4.1 Sécurité

Avant d'étudier la classification de la sécurité, nous allons nous intéresser aux facteurs la constituant.
Dans ce qui suit nous traiterons de l'aspect technique[6] et non juridique condamnant et réprimandant la fraude, malveillances volontaires avec pertes d'informations. Voici d'autres paramètres à prendre en considération :

Sensibilité de l'information
C'est le principal facteur de détermination du niveau de sécurité à adopter pour minimiser les risques sur un système d'information.

Conséquence d'une divulgation
Elle définit l'impact financier d'une perte de l'information et permet de traiter l'importance de l'information et donc le coût des moyens à mettre en œuvre pour la protéger.

[5] 🕮 ***Dependability : Basic Concepts and Terminology***, J.C LAPRIE, Dependable Computing and Fault-tolerant Systems, Volume 5, Springer-Verlag Wien New York, 1992
[6] 🕮 ***Computer Related Risks***, Peter G. NEUMANN, édition : Addison Wesley

Durée de vie de l'information
Une information a une durée de vie dans le temps (notion de pérennité de l'information dans le temps). Plus l'information tombera rapidement dans le domaine public, moins son niveau de sécurité devra être important.

Ces facteurs déterminés, nous pouvons classifier la sécurité de l'ensemble des ressources d'informations selon leur confidentialité, disponibilité et intégrité.

La confidentialité
Cette classification permet de déterminer l'impact d'une divulgation éventuelle pouvant engendrer une perte financière ou des dommages personnels.

La disponibilité
Cette classification indique le degré d'urgence des besoins de ces informations.

L'intégrité
Cette classification reflète la sévérité des dommages qui pourraient être causés par l'utilisation d'informations altérées.

2.4.2 Vulnérabilité

Pour définir ce terme, nous pourrions dire que tout ce qui peut être exploité pour obtenir un avantage aux dépens d'un tiers est une vulnérabilité.
Dans le cas d'actes malveillants, la vulnérabilité est une faiblesse exploitée par une menace pour provoquer des pertes ou des dégâts.
Cette faiblesse, vulnérabilité du système, est un point par lequel une erreur, un défaut ou une attaque peuvent rendre le système incapable de fonctionner de façon satisfaisante par rapport aux, fonctions pour lesquelles il a été réalisé.
Elle existe au niveau matériel mais aussi au niveau logiciel.
Nous allons voir quelques exemples de vulnérabilités les plus courantes :

Point faible dans la conception de la sécurité
Nous traitons ici les fautes de conception comme par exemple faire circuler un mot de passe non chiffré sur le réseau.
Cette faiblesse peut être due à une analyse de la sécurité ne traitant pas de cet aspect de la sécurité ou à un événement imprévu survenant lors de la mise en production mais sur lequel aucun test révélant ce type de problème n'a été fait.

Implémentation défectueuse
Elle provient d'une installation ou d'une administration défectueuse.
Lors de l'installation ou de l'administration du système d'information, les paramètres par défaut ne sont pas systématiquement conformes aux exigences de sécurité du cas étudié.

Utilisation abusive non prévue
Le système fonctionne dans un état non prévu à l'origine lors de sa conception. Par exemple, un événement survient alors qu'aucun remède n'a été prévu à sa conception.

Action psychologique
Astuce ou stratégie obligeant un individu à divulguer des informations qu'il devrait taire. Le seul moyen de réduire cette vulnérabilité est de faire suivre au personnel une

formation et de l'informer sur la sensibilité des données qu'il manipule ou dont il a connaissance dans l'entreprise.

2.4.3 Causes et effets

La *cause* est *ce qui fait qu'une chose est ou se fait* - ce par quoi une chose existe. Elle est l'origine d'un *effet* produit - *résultat d'une action*[7].

Les notions de causes et effets sont importantes dans tout système complexe ou non. Si un élément de la chaîne présente un aspect défectueux, celui-ci peut rendre le système global inutilisable, voire le stopper complètement.

Etapes de construction du diagramme causes-effets

Il y a des synonymes : arbre d'*Ishikawa*, diagramme en arrêtes de poisson, *Fishbone diagram*. Cet outil graphique de production d'idées se construit comme suit :

- Définir *l'effet* à observer :défaut, caractéristique du produit ou du procédé
- Tracer une flèche de gauche à droite en direction de l'effet.
- Décrire les facteurs principaux qui sont les causes potentielles de ce qui est observé.

La recherche des *causes* peut se faire selon les **5M** : *Main d'œuvre, Matière, Méthode, Machines* (équipement), *Milieu* (environnement). Nous pouvons y ajouter deux autres "**M**" pour arriver à **7M** : *Management* et *Moyens financiers*, qui constituent des facteurs intéressants, notamment dans les domaines immatériels, les services, gestion de projets, logiciels par exemple.

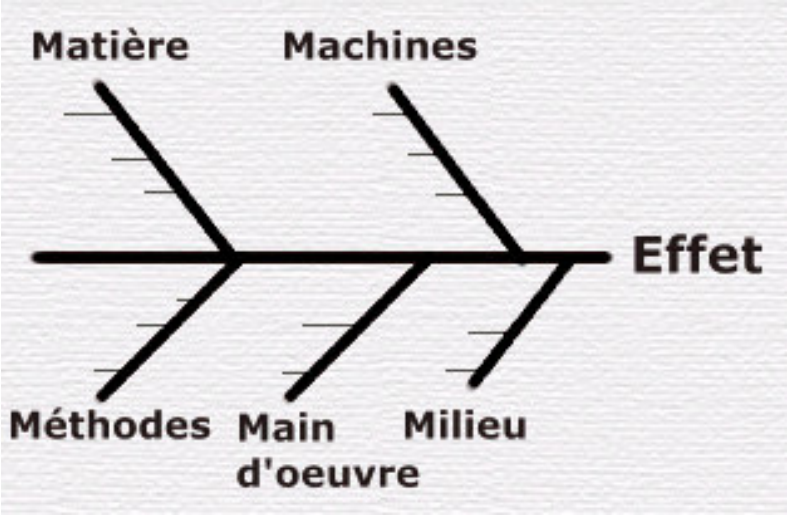


Figure 7 - Diagramme Causes-Effets[8]

A titre d'exemple, nous présentons ci-dessous plusieurs causes :

- causes à *événement unique*
- causes *multiples indépendantes*
- causes *multiples simultanées*

[7] 🕮 Source : Dictionnaire *Larousse* et Dictionnaire *Hachette*
[8] 🕮 Source : http://www.multimania.com/hconline/top

Les causes à événement unique

Ecrasement d'un DC10
Un DC10 de la compagnie American Airlines s'est écrasé suite à un défaut d'indicateur d'alerte cabine. Ce défaut est survenu suite à une faiblesse du câble venant de l'un des moteurs. Dans ce cas, un simple câble défectueux est la cause de la panne de l'indicateur et les effets ou conséquences lourdes de ce défaut est l'écrasement de l'avion.

Les causes multiples indépendantes

Tests d'erreurs indépendantes
Pendant la 2nd guerre mondiale, un concepteur de bombardier Handley Page a utilisé trois méthodes de preuves indépendantes dans son avion :, pour analyser l'efficacité des stabilisateurs de queue.
Chacune des trois preuves montrait la même erreur. Par coïncidence, elles existaient toutes sur le même avion.

Les causes multiples simultanées

La navette Discovery
Les concepteurs du train d'atterrissage ont ignoré la possibilité de défauts simultanés. Lors de son retour sur terre, le 19 avril 1985, le train d'atterrissage présentait des problèmes fonctionnels importants.
L'un des éléments de la roue principale était fermé à clé, l'un des pneus était râpé et l'autre sous gonflé.
En janvier 1982, le responsable de la sécurité de l'Aérospatiale avait signalé une usure pouvant engendrer un sinistre.
En effet, les deux pneus côté droit de la navette avait un problème simultanément.
D'autre part, en janvier 1983, lors d'un contrôle, il a été signalé un affaiblissement du train d'atterrissage ainsi qu'au système de freinage.
Autant de coïncidences qui auraient dû alerter les services de sécurité pour interdire le lancement.
De ces types d'exemples, les littératures en sont remplies.

Parmi les diverses causes, nous pouvons distinguer deux grandes familles :

- les causes *intentionnelles*
- les causes *accidentelles*

Les causes *intentionnelles* peuvent être causées par des personnes internes à l'entreprise dont les fonctions peuvent être diverses: dessinateurs, intégrateurs, mainteneurs, opérateurs, utilisateurs, ou même des individus externes à l'entreprise : prestataires, sous-traitants, experts, consultants, entreprises concurrentes.

Les causes *accidentelles* peuvent être causées par la même catégorie d'individus mais de façon involontaire.
Il devient alors difficile de discerner un acte intentionnel d'un acte accidentel.

2.5 Modélisation et évaluation des risques

2.5.1 Modélisation de la sûreté de fonctionnement

Dans un projet donné, il est utile d'énumérer les différentes formes de risques possibles sur le système d'information. Néanmoins, la liste d'énumérations de ces risques varie selon l'entreprise, voire l'individu qui l'établit.

Toutefois, un certain nombre de notions reviennent systématiquement :

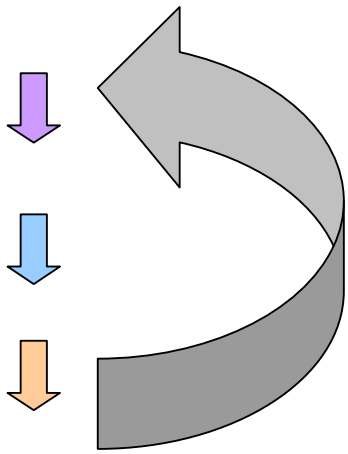
- la *sûreté*
- la *défaillance*
- la *sécurité*
- la *performance*
- la *tolérance aux pannes*

Dans un premier temps, nous allons voir le modèle lié à la sûreté d'un système d'information.

2.5.2 Modèle de la sûreté de fonctionnement

Cette notion est liée à la qualité du service délivré. Le modèle de base[9] permettant de formaliser cette notion de sûreté est composé de trois entités principales :

1. *Défaillance*
   Evénement survenant lorsque le service délivré n'est plus conforme à la spécification. Transition de service correct vers service incorrect.
2. *Faute*
   Cause adjugée ou supposée d'une erreur. Cause d'erreur évitée ou tolérée. Conséquence de la défaillance d'un composant pour le système qui le contient ou pour le ou les composants qui interagissent avec lui.
3. *Erreur*
   Partie de l'état d'un système par rapport au processus de traitement qui est susceptible d'entrainer une défaillance. Manifestation d'une faute dans un système[10].



La *défaillance* d'un système d'information survient quand le service délivré diffère du service spécifié préalablement.

Une *erreur* est la partie de l'état pouvant engendrer une défaillance. Une erreur peut entraîner d'autres erreurs résultantes.

Une *faute* est la cause physique d'erreur avérée.

[9] 🕮 ***Dependability : Basic Concepts and Terminology,*** J.C LAPRIE, Dependable Computing and Fault-tolerant Systems, Volume 5, Springer-Verlag Wien New York, 1992, page 64.

[10] 🕮 ***Dependability : Basic Concepts and Terminology,*** J.C LAPRIE, Dependable Computing and Fault-tolerant Systems, Volume 5, Springer-Verlag Wien New York, 1992, page 85, 86, 87.

Lorsqu'une erreur a un impact sur le service délivré, une défaillance survient.
A ce niveau de fonctionnement se pose le problème de la sûreté de fonctionnement.
Nous distinguons plusieurs types de fautes d'origines diverses :

Faute physique : C'est une faute perturbant l'environnement du système d'information. Ce type de faute apparaît lors d'un phénomène physique interne ou externe à l'environnement.

Faute humaine : Défaut de conception, de réalisation, faute d'interactions dues à des violations volontaires ou accidentelles des procédures d'exploitation ou d'utilisation.

La manifestation de plusieurs fautes dans un environnement système va entraîner une erreur et plusieurs erreurs, une défaillance.

De ce fait, nous distinguons plusieurs modes de défaillances :

- *Défaillance sur les valeurs* : restitution ou délivrance de résultats erronés.
- *Défaillance dans le temps* : valeur restituée dans des délais non conformes aux exigences du système.

Ce problème est très important dans les concepts temps réels en particulier.
Selon la gravité des conséquences d'une défaillance, celle-ci peut être inacceptable ou au contraire tolérable.

2.5.3 Arbres de défaillances

Le principe des arbres de défaillances est basé sur la récursivité du phénomène de panne. Le modèle défini précédemment peut s'appliquer à un élément du système en y intégrant une analyse des conséquences de la défaillance de ces éléments sur le système global[11].
Nous pouvons donc mettre en évidence, par ce procédé, qu'une défaillance d'un élément est une faute pour le sous système intégrant cet élément et la défaillance de ce sous système une faute pour le système global.
Dans cette approche, en partant de la conséquence critique, nous pouvons remonter l'arbre en déterminant le ou les événements la provoquant, puis remonter successivement jusqu'à obtenir les événements déclencheurs du sinistre.

Pour chaque événement, nous essaierons de déterminer la probabilité d'occurrence, permettant ainsi de calculer la probabilité du sinistre la plus critique.
Le calcul de probabilité sur un événement n'est pas toujours possible (cas de défaillances dues à des événements liés à l'environnement), c'est pourquoi ce type de méthode fait appel à des jugements raisonnés, permettant de mobiliser des valeurs personnelles en fonction du cas étudié.
Cette approche donne des résultats intéressants dans les cas d'analyses de risques.

2.5.4 Moyens de la sûreté de fonctionnement

Méthodes, outils et solutions permettent de fournir au système les moyens de délivrer un service conforme aux spécificités d'origines.

[11] 🕮 ***Serveurs multiprocesseurs clusters et architectures parallèles***, René CHEVANCE, édition : Eyrolle, 2000, page 416.

Prévention des fautes :

- Empêcher ou minimiser l'apparition d'une faute
- Tolérance aux fautes : délivrer un service conforme aux exigences malgré l'apparition d'une faute.

Ces deux moyens permettent d'assurer l'obtention de la sûreté de fonctionnement.

Les mesures auxquelles nous avons recours pour assurer cette sûreté :

- *Elimination* des fautes par suppression des erreurs, minimiser la survenance et la présence de fautes.
- *Prévention* des fautes par estimation, évaluation, présence et conséquences d'une faute.

Ces deux derniers moyens peuvent être vus comme la validation de la sûreté de fonctionnement.

2.5.5 Attributs de la sûreté de fonctionnement

La sûreté de fonctionnement est mesurée selon les indicateurs suivants :

- *Disponibilité*
- *Fiabilité*
- *Sûreté*
- *Sécurité*

La mesure des attributs dans ce modèle est fortement attachée à des notions de fiabilité ou probabilité de délivrance d'un service conforme aux attentes.

2.5.6 Objectif décisionnel du modèle

A ce niveau de l'analyse, deux objectifs majeurs apparaissent :

- Sensibiliser la *direction de l'entreprise*
- Définir un *schéma directeur* pour remédier à ces risques

Le résultat de cette analyse engendre une proposition pour de nouveaux investissements généralement importants.

Une remise en cause régulière (au moins tous les six mois) de ce modèle devra être faite afin de minimiser les conséquences des risques face à de nouveaux risques : problème de la pérennité des moyens mis en œuvre.

2.5.7 Analyse fonctionnelle des solutions de sécurité

L'objectif est de définir les spécifications fonctionnelles des solutions de sécurité adaptées au contexte étudié :

- Consolider ces analyses pour créer un schéma d'ensemble cohérent
- Justifier la nécessité de ces mesures aux utilisateurs du système d'information concerné.

2.5.8 Analyse Opérationnelle

Deux objectifs majeurs pour ce type d'analyse :

- Déterminer les *solutions* à mettre en œuvre : nous décrivons dans cette analyse les mécanismes de solutions offertes
- Former les *responsables sécurité* et opérationnels chargés de la bonne mise en œuvre

2.5.9 Schéma directeur de la sécurité du système d'information:

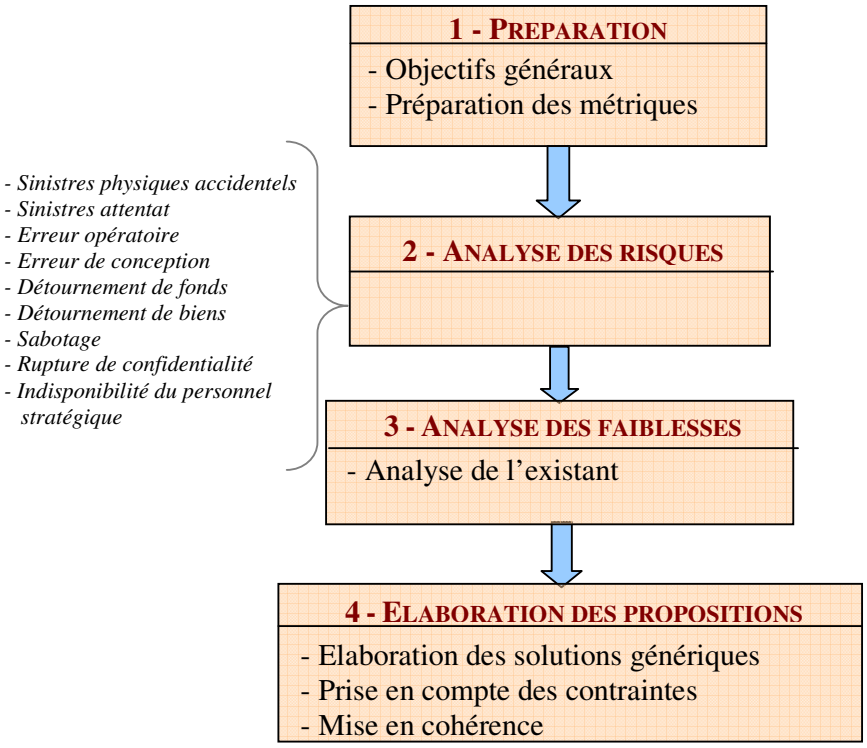


Figure 8 - Schéma directeur de la sécurité du système d'information

2.5.10 Evaluation des risques

Dans ce chapitre, nous allons voir comment mesurer le risque en fonction de divers paramètres.
La gravité d'un sinistre est essentielle. Elle est définie par l'impact.
Deux formes d'impacts existent :

- L'*impact intrinsèque* pour lequel il n'y aura aucune parade
- L'*impact effectif* pour lequel il existe une parade, pouvant être mise en place

D'autre part, le risque peut être courant ou exceptionnel et, à impact équivalent, nous pouvons attacher une plus grande importance à des risques courants plutôt qu'exceptionnels.
Ce paramètre sera défini par la potentialité.
Nous pourrons parler de potentialité tant que l'agression n'a pas engendré de détérioration.
Dans le cas où le sinistre aurait déjà engendré une détérioration, nous parlerons de gravité du sinistre nécessitant la mise en œuvre de mesures de protection, de sécurité ainsi que toutes les mesures palliatives visant à réduire, minimiser, récupérer les données afin de remettre en fonctionnement le système d'information impacté.

2.5.11 La Potentialité

Le problème de la potentialité est de définir une pondération par rapport au risque correspondant.
La potentialité va être un jugement de la personne effectuant l'étude du risque associé.
En effet, tout le monde est assuré contre certains risques mais peu de personnes prévoient un abri antiatomique par exemple!

Il y a donc une prise de connaissance des risques permettant de distinguer ceux qui seraient réels de ceux éloignés et/ou peu probables ne nécessitant pas d'investissements disproportionnés pour assurer une protection trop importante.

Les niveaux de potentialité

Selon la méthode d'analyse du risque utilisée, nous pouvons constater un nombre de niveaux de potentialité différents.
Dans la méthode de MARION, seul deux niveaux sont définis : un scénario est potentiel ou ne l'est pas. Par exemple, la destruction d'un centre informatique, de son « backup » et du « backup du backup » semble peu probable dans cette méthode et n'est donc pas prise en compte.
Dans la méthode CRAMM[12] ; nous observons par contre trois niveaux : fort, moyen, faible ou insignifiant. Elle semble être plus réaliste dans son approche de la potentialité plutôt que la méthode MARION qui élimine d'emblée une certaine catégorie de risques.
Elle est néanmoins très lourde et est adaptée à de grosses entreprises uniquement. CRAMM est une méthode d'analyse de sécurité imposée par le gouvernement britannique.

Potentialité forte

Nous définirons par ce type de potentialité ceux qui font partie de la vie courante de l'entreprise, ceux dont nous sommes sûrs des conséquences compte tenu de l'environnement dans lequel le risque peut être amené à évoluer.
Par exemple, cette potentialité va prendre en compte les actions humaines dont les conséquences évidentes seront fortes si aucun remède n'est apporté à temps.

Potentialité moyenne

Ce sont les scénarios qui ne font pas partie de la vie courante mais dont nous estimons qu'ils peuvent probablement arriver, sur un événement donné.
Nous retrouverons dans cette catégorie de potentialité les évènements naturels.

Potentialité faible

Les scénarios intégrant cette potentialité sont ceux que nous considérons comme exceptionnels mais qui restent possibles.
Dans cette catégorie, nous aurons les événements qui apparaîtront uniquement grâce à des concours de circonstances exceptionnels.
Nous pouvons citer dans cette catégorie l'événement du 11 Septembre 2001 aux USA, intégrant le fait qu'un avion pouvait s'écraser sur une tour du World Trade Center en plein New York. La potentialité était faible. Potentialité encore plus faible pour qu'un deuxième avion s'écrase sur la seconde tour, surtout pratiquement au même instant ! Le fait que les deux tours soient effacées de la carte de cette ville n'était même pas pensable avant cela.

La méthode assimile une potentialité nulle à une potentialité insignifiante.
En d'autres termes, une potentialité n'est jamais nulle.

2.5.12 L' impact

L'impact d'un scénario nécessitera la restauration des données de l'entreprise.
Evaluer l'impact des détériorations signifie estimer le coût de restauration.
Tout comme la potentialité, l'impact est classifié en niveaux de gravité.

[12] CRAMM : *CCTA Risk Analysis and Management Methodology*:

Impact extrêmement grave
Nous intègrerons dans cette catégorie les cas où l'avenir de l'entreprise ou d'un de ces services est remis en cause.
C'est le cas où la disponibilité du système d'information est vitale pour l'entreprise.
Par exemple, si le système d'information n'est pas sauvegardé et que la survie de l'entreprise en dépend..

Impact très grave
Il s'agit d'un sinistre ayant un impact très sérieux sur le fonctionnement de l'entreprise mais sans menacer son avenir (perte de l'image de marque de l'entreprise par exemple).

Impact moyennement grave
Cet impact relève de tous les sinistres ayant un impact certain sur l'entreprise pouvant nuire à son image de marque, entraînant un impact certain sur ses résultats.

Impact peu grave
Cette classe définit les sinistres pour lesquels la divulgation ne constituerait pas un sinistre véritable pour l'entreprise, mais que l'on souhaite tout de même éviter.

Avant de clore ce chapitre sur l'impact, il faut souligner deux autres types d'impacts également utilisés.

Impact intrinsèque
C'est l'impact d'un sinistre défini en fonction des principes vus précédemment, sans tenir compte des moyens de dissuasion, de prévention, de protection, palliatives ou de récupération à mettre en place.
Nous cherchons à évaluer le pire si aucun moyen n'est mis en place pour remédier à une menace ou si les moyens présents se révèlent inefficaces voire inexistants.
C'est ce niveau d'impact, sa gravité, qui doit servir de base à la classification des informations et des ressources de l'entreprise.

Impact effectif
Ici, contrairement à l'impact intrinsèque, nous allons tenir compte des moyens de protections et des palliatifs dont l'efficacité peut être garantie.

2.6 Mise en évidence des types de risques par l'exemple

Nous vous présentons ci-dessous un certain nombre d'exemples de risques informatiques[13] associés aux types de risques définis dans le chapitre *Typologie* ainsi que leurs conséquences.

Exemple associé au risque de Type A1
Rupture d'un câble de fibre optique : En juillet 1991, une société de San Francisco voit son réseau de fibre optique coupé, affectant ainsi ses services longues distances. AT&T, responsable de ce service, ''reroute'' cette ligne défectueuse sur une autre ligne, provoquant un engorgement du réseau (goulet d'étranglement).

[13] Selon la classification de l'APSAD (*Assemblée Plénière des Sociétés d'Assurances Dommages*).

Exemple associé au risque de Type A4

Rupture d'un câble en Virginie (USA) : En juin 1991, une entreprise de travaux publics coupe deux câbles parallèles informatiques d'une agence de presse avec l'un de ses engins, isolant l'agence située en Angleterre de son réseau ARPANET.

Exemple associé au risque de Type E1

Missions Voyager : Pendant un week-end, Voyager 1 a perdu les données de sa mission à cause de ses cinq imprimantes. En effet, quatre d'entres-elles n'étaient pas configurées correctement et la dernière présentait un problème de bourrage papier. Toutes les données envoyées furent perdues définitivement.

Exemples associés au risque de Type E2

Rapport de crash d'un avion militaire : Un chasseur F-18 s'est écrasé à cause de la programmation de l'un de ses instruments de bord : une condition "IF … THEN" sans clause' ELSE '. Cette instruction pilotait la mise à feu d'un missile chargé sous l'avion et cette omission a entraîné la chute de 20 000 pieds de l'appareil qui aurait dû larguer son armement normalement.

Bug logiciel Mercury : Voici l'un des problèmes de l'informatique les plus connus dans un programme Fortran. Une ligne de programme a été saisie DO I = 1.10 au lieu de DO I = 1,10 entraînant une erreur de syntaxe fatale lors de l'exécution de cette ligne. Ce programme était fonctionnel lors de précédentes missions spatiales, mais ne passait pas par cette ligne d'instruction. Le programme a été porté sur une nouvelle mission, l'événement s'est malheureusement produit et a généré l'arrêt du déroulement du logiciel.

Calcul sur les dates : En 1992, une personne âgée de 104 ans reçoit une invitation pour assister à un jardin d'enfant avec d'autres personnes nées en 88. L'utilisateur de ce système a effectué une requête sur sa base de données en saisissant 1988 pour ne prendre en considération que les personnes nées depuis cette date, mais le logiciel ne prenait en compte que les deux derniers chiffres.

Vainqueur d'une loterie : En janvier 1990, le vainqueur d'une loterie n'a pu être déterminé que 3 jours après le tirage pour cause de programme défectueux dans le tirage des numéros.

Logiciels non portables : Un programme, développé aux Etats Unis pour modéliser l'espace aérien à contrôler, a été voué à l'échec quand il a été essayé en Angleterre. Le programme ne prenait pas en compte l'Est des longitudes de Greenwich.

Autant d'exemples qui mettent en évidence l'importance et la nécessité de bien mesurer les risques pouvant survenir lors d'une mission ou d'un projet.

Afin de mieux comprendre ces phénomènes laissés plus ou moins à l'écart dans les sociétés d'hier et d'aujourd'hui, nous allons voir dans le chapitre suivant comment analyser, mesurer, et modéliser le risque. Un chapitre sera consacré aux techniques permettant de limiter ces risques souvent aux graves conséquences financières, matérielles ou bien pire encore, humaines.

2.7 Analyse des risques

Cela consiste à réaliser une étude des dommages qu'un risque pourrait causer et de calculer la probabilité de survenance d'un incident lié à un défaut de sécurité.
La base de l'analyse du risque est de déterminer un niveau de sécurité nécessaire pour justifier l'investissement, sécuriser un système d'information et comprendre les impacts sur le matériel, les informations de la société et enfin évaluer l'impact financier engendré par un éventuel incident.

2.7.1 Evaluation de l'exposition naturelle

Nous désignons par cette évaluation les expositions à une agression par analyse des enjeux pour un agresseur humain.

2.7.2 Evaluation du risque de l'agresseur

C'est une évaluation sur la base des possibilités de remonter à l'auteur de l'agression et des sanctions qui pourront être prises.

2.7.3 Evaluation de la force de l'agresseur

Compte tenu des solutions en place, la force d'agression doit avoir un niveau minimal pour aboutir. C'est le rôle des algorithmes de déterminer ce niveau pour un cas donné ou des obstacles mis en place afin d'empêcher la réalisation de la menace.

2.7.4 Evaluation de la potentialité

A ce stade de l'analyse, nous porterons un avis critique sur la potentialité obtenue et la mise en place de processus de correction.
Dans cette évaluation, une analyse sera développée sur la notion de malveillance.

2.7.5 Evaluation de l'impact

Pertes liées aux dégâts

Ce type de perte va permettre d'évaluer les dégâts engendrés par la détérioration sur le système d'information. Elle est fonction de la gravité des conséquences ou de l'impact. Il faut donc faire attention à prévoir toutes les conséquences possibles et retenir le pire.

Pertes liées aux détériorations

La restauration et/ou reconstruction de fichiers détériorés a un coût financier.
La restauration, en particulier dans des domaines pointus (rareté de la compétence), est la seule à pallier les destructions accidentelles. Le coût de la restauration peut avoir un impact grave pour l'entreprise.

Mesure de l'impact

Nous allons mesurer ici le caractère plus ou moins supportable des conséquences.
Nous allons considérer la durée et le niveau de perturbation créés dans l'entreprise.
Un impact grave peut correspondre à une perturbation majeure.

2.8 Risques dans l'analyse des risques

Dans ce chapitre, nous allons essayer de mettre en évidence quelques-uns des risques inhérents à l'analyse des risques.
En fait, le risque dans cette analyse est l'exactitude ou l'inexactitude de l'information recueillie.

Une inexactitude mineure pourra être tolérable. Par contre, à une inexactitude signifiante pourront correspondre des conséquences importantes sur le système d'information.
D'autre part, il ne faut pas tomber dans l'excès aussi bien en terme de coût financier qu'en terme d'effort.
Mais où s'arrête la limite en matière de risque de ne pas exploiter une nouvelle opportunité ?
A l'inverse, si le risque est sous estimé, nous aurons à faire face à des événements imprévus dans l'analyse et à remédier à des événements en flux tendus.

Le deuxième risque majeur est d'effectuer une analyse trop parfaite.
Ce type d'analyse peut être résumé par un exemple.
Après avoir pris toutes les mesures contre le terrorisme et avoir envisagé toutes les solutions, ce n'est pas parce que l'acte terroriste ne se produit pas que le terrorisme est stoppé.

Une forme de risque consiste à utiliser l'analyse du risque comme une forme d'intimidation et non pas comme un outil permettant d'améliorer une situation à risque.

Le quatrième risque est de compter sur l'analyse humaine et sur le bon sens des résultats. S'il y a des analyses concurrentes sur un résultat, l'analyse peut porter sur la concurrence de ces méthodes plutôt que sur les résultats obtenus et sur ce qu'ils peuvent représenter.

Le dernier risque est d'utiliser trop finement l'analyse des risques empêchant ainsi toute évolution d'un projet.
En effet, un résultat peut être perçu comme une prise de risque et la progression du projet peut se voir freinée.

D'une manière générale, selon les études effectuées sur le sujet, il a été constaté qu'il n'y a que peu de contrôles de la qualité sur l'analyse des risques.
Il n'y a aucune certitude sur l'apparition d'un événement.
La devise de l'ordre des médecins me paraît intéressante et peut être rapprochée de l'analyse des risques : « En premier lieu, ne faîtes aucun mal ».
La difficulté est de juger le niveau d'analyse par rapport à une situation donnée.

2.9 Méthodes de mesure des risques

L'objectif de la mesure des risques est d'identifier les méthodes et apporter des solutions pragmatiques et palliatives à un sinistre éventuel parmi lesquelles les méthodes EBIOS, FEROS, MARION et MEHARI.

2.9.1 Méthode EBIOS

Tout d'abord, un bref commentaire par rapport à la méthode EBIOS utilisée par la défense nationale Française.
Nous verrons que parfois cette méthode est limitative dans certaines circonstances compte tenu du concept sur lequel elle repose.
En effet, elle considère R le *risque* comme étant le produit de la *probabilité* d'avoir un sinistre P par la *gravité* de l'impact provoqué I.

$$R = P \times I$$

Si nous considérons un impact très fort avec une probabilité forte le risque sera fort.

Prenons l'exemple du 11 septembre 2001 à New York.
Le seul fait qu'un avion s'écrase sur la première tour avait de très faibles probabilités d'arriver et encore plus le fait que le deuxième avion s'écrase sur la deuxième.
Quant à l'effondrement des deux tours cela n'aurait pas dû arriver.
Néanmoins l'impact est très important compte tenu des conséquences que nous connaissons.
De plus, pouvons nous modéliser le risque par une équation mathématique ?
Si nous regardons cette formule, si l'une des composantes, la probabilité ou l'impact, est faible la résultante sera faible, ce qui voudrait dire que le risque est minime.
Nous allons voir d'autres méthodes permettant de mieux refléter la réalité des choses.

2.9.2 Méthode FEROS

L'objectif de cette méthode est de favoriser la sécurité du système d'information.
Selon cette méthode, ceci semble être obtenu de façon cohérente et relationnelle par une étude minutieuse des enjeux et des contraintes.
Lors du développement d'un système d'information, la disponibilité est souvent prise en compte mais rarement la confidentialité et l'intégrité des données.
Cette méthodologie oblige, pour les systèmes d'information appelés à traiter des données faisant l'objet d'une classification de défense, de mettre en place la rédaction d'une Fiche d'Expression Relationnelle des Objectifs de Sécurité : FEROS.
Elle permet de connaître les objectifs de sécurité adaptés aux besoins.
La rédaction d'une telle fiche empêcherait une prise en compte tardive des besoins de sécurité et conduirait forcément à des surcoûts ainsi qu'à des baisses réelles de performances.
Les méthodes EBIOS et FEROS ne prennent pas en compte l'ensemble des notions de risques d'un système d'information et sont visiblement orientées dans leurs démarches.

2.9.3 Méthode MARION

La méthode MARION a été mise au point par le CLUSIF il y a quelques années.
Moins complète que la méthode MEHARI comme nous le verrons dans le prochain paragraphe, elle est plus rapide à utiliser et permet de faire une photographie de l'état de la sécurité d'un système d'information à un instant donné.
Basée sur des questionnaires élaborés par le CLUSIF et remis à jour à intervalles réguliers, ces questionnaires prennent en compte 27 facteurs de sécurité, couvrant notamment :

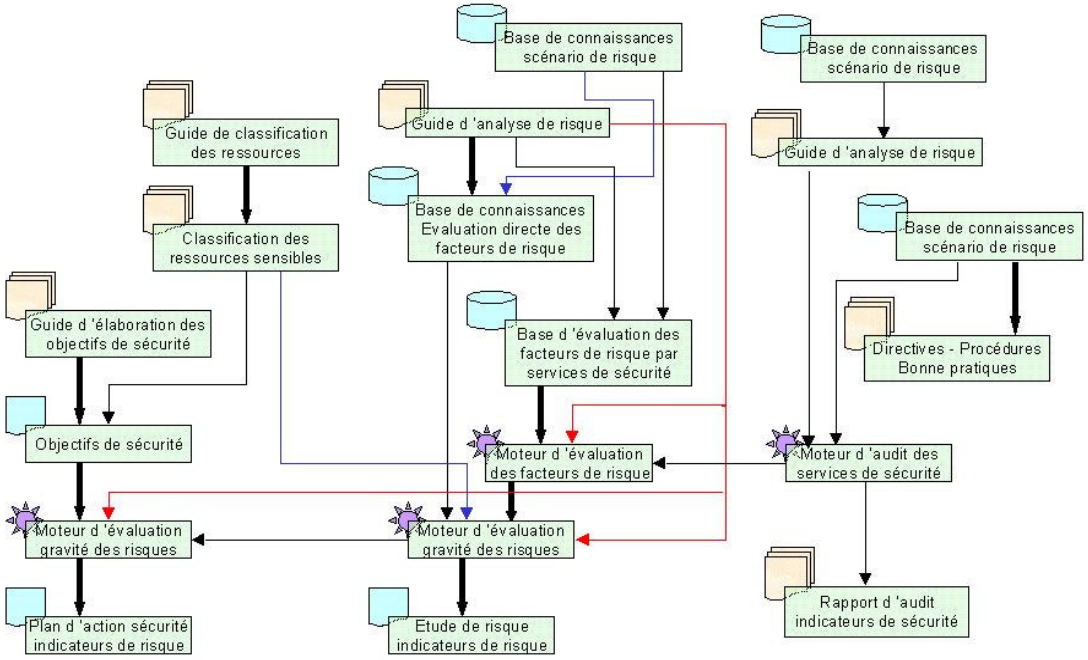
- l'organisation
- l'environnement technique
- la sécurité des télécommunications
- les sauvegardes
- les relations utilisateurs et informaticiens

Pour les entreprises faisant l'objet de ces questionnaires, leur système d'information sont identifiées au travers de trois environnements distincts:

- les grands sites
- les PME/PMI
- la micro-informatique

En fonction du résultat obtenu par ces questionnaires, nous pouvons établir des constats, dont peuvent être déduits des plans d'action de sécurité précis.

2.9.4 Méthode MEHARI



démarche complète de la méthode MEHARI

Figure 9 - Méthode MEHARI

Explications

La méthode MEHARI résulte des travaux de Jean-Philippe JOUAS et de Albert HARARI . La commission Méthodes du CLUSIF en a fait la consolidation.

Sur la base de ce modèle et en incorporant le savoir-faire ainsi que les bases de connaissances acquises par le CLUSIF depuis 1984 avec la méthode MARION, s'est construit depuis un ensemble d'outils de management de la sécurité appelé MEHARI (Méthode Harmonisée d'Analyse du Risque Informatique).

Cette boite à outils peut donner, en fonction des besoins et des circonstances, une solution au problème posé de management de la sécurité.

La méthodologie comprend les éléments suivants :

1. *guides*
2. *bases de connaissance*
3. *moteurs* ou *processus d'évaluations quantitatives*

Mode d'utilisation

On constate un fait et plusieurs actions sont opérées :

- *Collecte* des données fournis lors d'un audit du système d'information fait sur le terrain
- *Consultation* de la base de connaissance pour trouver un scénario possible
- *Rapprochement* par recherche algorithmique dans le moteur d'évaluation d'un risque correspondant

De cette façon, une solution opérationnelle et palliative est déduite.

Dans la méthode MEHARI, un algorithme de recherche est utilisé. A la différence de la méthode EBIOS disant que **R = P x I**, il n'y a pas ici d'équation mathématique. Nous pouvons constater que la méthode est basée sur de nombreuses simulations en fonction des paramètres de risques entrés.

Guide de classification des ressources sensibles
Ce document est destiné aux managers souhaitant entreprendre une échelles des ressources sensibles sans l'aide de spécialistes.
Les critères pris en compte sont les :

- *critères* de classification
- *niveaux* de classification (nombre et définitions)
- *processus* de classification (description, modèle de tableaux, étape du process)

Guide d'audit des services de sécurité
Ce document est destiné au responsable de la sécurité du système d'information et aux membres de son équipe.
Ces audits sont des diagnostiques de sécurité du système d'information.
Les points traités dans ce guide sont :

- les *objectifs* de l'audit
- le périmètre :
- types et limites des systèmes d'information, sites et entités concernés
- le *référentiel* de l'audit :
- les éléments de référence, les procédures internes de sécurité, finesse de l'audit
- les *acteurs* et *intervenants* de l'audit
- le *processus* et la *méthodologie* de l'audit

Guide d'analyse de risque
Ce document est destiné au responsable de la sécurité des systèmes d'information, aux membres de son équipe et aux opérationnels amenés à effectuer ce type d'analyses.
Les points traités dans ce document sont :

- les *objectifs* et les *limites* de l'analyse de risque
- l'élaboration des *référentiels* servant de bases à la métrique de risque
- le choix de *scénarios* de risque adaptés au contexte et à l'entreprise
- les *processus* et les *méthodes* d'évaluation
- les *acteurs* et *intervenants* de l'analyse, experts et groupe de pilotage

Guide d'élaboration d'objectifs de sécurité
Ce document est destiné au responsable de la sécurité des systèmes d'information qui souhaiterait entreprendre seul la détermination des objectifs de sécurité.
Il décrit :
le fondement de ces objectifs pour faire définir par la direction des catégories de risques tolérables, inadmissibles, insupportables et de transformer cette décision de nature politique en objectifs de sécurité utilisables par les responsables de la sécurité.
le processus d'élaboration de ces objectifs
une base de scénarios de risques type pouvant servir de support à ce processus.

Base des services de sécurité
Cette base de connaissances décrit l'ensemble des services de sécurité.

Ces services de sécurité sont toujours décrits en termes fonctionnels et n'incluent jamais les mécanismes permettant de réaliser la fonction.

Bases d'audit des services de sécurité
Ces bases de données regroupent un ensemble de questions pertinentes quant à la qualité du logiciel et quant à la qualité des services de sécurité.
A ces questions sont associés des éléments de pondération au moteur d'évaluation de la qualité des services de sécurité que nous verrons plus loin dans ce chapitre.

Base de connaissance - scénarios de risque
La base des scénarios de risques contient un ensemble de scénarios de risques classés par famille de conséquences.
Nous préciserons pour chaque scénario un certain éléments tels que le type de vulnérabilité, le type d'acteur ou l'origine du scénario. Seront également abordés les problèmes de disponibilité, d'intégrité, et de confidentialité du système d'information.

Base d'analyse des scénarios de risque en fonction des services de sécurité effectifs
Cette base indique pour chaque scénario les services de sécurité pouvant avoir un effet sur le niveau de risque résultant.

Base d'analyse des scénarios de risque par évaluation directe des facteurs de risque
Cette base permet l'analyse des scénarios de risque par une évaluation des facteurs de risque.

Moteur d'évaluation de la qualité des services de sécurité
Ce moteur permet, en fonction des réponses apportées lors de l'audit des services de sécurité, de fournir une évaluation globale de chaque service sous la forme d'une note de qualité de service.
Les facteurs entrant en considération pour l'attribution de cette note sont :

- Une *moyenne pondérée* de l'ensemble des questions relatives au même service de sécurité.
- La limitation du *niveau de qualité* si certaines réponses fournies sont négatives
- L'obtention d'un *niveau minimal* pour les réponses positives.

Moteur d'évaluation des facteurs de risque
Le moteur fournit une évaluation des facteurs de risque pour chaque scénario, en fonction de la qualité des services de sécurité appelés par la base des scénarios de risques.

Moteur d'évaluation de la potentialité et de l'impact d'un scénario de risques
Ce moteur permet de fournir, en fonction des évaluations de facteurs de risque et de la classification de la ressource concernée par le scénario, une évaluation de la potentialité et de l'impact du scénario de risques.

Moteur d'évaluation de la gravité d'un risque
Ce dernier moteur permet de passer des évaluations de la potentialité et de l'impact à une évaluation globale de la gravité du risque.

2.10 Outils d'analyse des risques

Ai-je un réel besoin en matière de sécurité informatique ?
Telle est la question pour justifier et argumenter sur un investissement auprès des financiers d'une entreprise.

Parmi mes différentes recherches, j'ai pu trouver deux outils permettant d'effectuer des analyses de risques fiables.
Ces outils vont nous permettre d'analyser et d'effectuer un suivi de l'évolution de la sécurité informatique.

2.10.1 Risicare

RISICARE permet de réaliser une analyse de risques liée au système d'information.
L'utilisation de la méthode MEHARI, développée au sein du CLUSIF, comme modèle d'analyse, garantit la pérennité de la démarche et ses capacités d'évolution future.

Concrètement l'analyse se déroule en trois phases :

- Un *audit* de l'existant avec un ensemble de questionnaires réellement adaptés aux parties de l'entreprise étudiées.
  Cet audit conduit à des tableaux de cotations et de nombreuses représentations graphiques permettant un reporting et un suivi de la vulnérabilité d'une organisation.

- La mise en évidence de *scénarios de sinistres* et la quantification automatique de leur gravité à partir de l'audit précédemment réalisé. RISICARE, par des codes couleurs associés, permet de voir immédiatement les failles de sécurité les plus significatives et leur localisation.

- La construction d'un *plan d'action* visant à réduire la gravité des scénarios de sinistres les plus critiques.
  Cette phase peut être vue comme une véritable simulation d'actions à entreprendre, RISICARE donnant immédiatement leurs influences sur la gravité des scénarios de sinistres.
  L'analyse sera conduite par le client final, utilement assisté d'un spécialiste (en fonction de son niveau de connaissances de la méthode MEHARI).

2.10.2 Analyse des Effets des Erreurs sur le Logiciel (AEEL)

AEEL est issue de l'AMDEC (Analyse des Modes de Défaillances, de leurs Effets et de leur Criticité) intégrant la notion de sûreté de fonctionnement dès les premières étapes du cycle de vie[14].

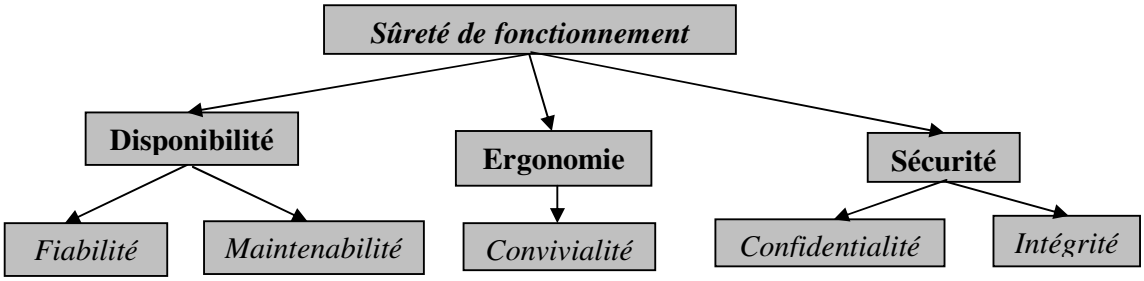


Figure 10 - Cycle de vie

L'objectif est de déterminer les fonctions critiques, identifier les défaillances critiques, adapter les niveaux de tests, prévoir des solutions.

[14] 🕮 Source : *Institut des Sciences et Techniques de l'Ingénieurs d'Angers* (ISTIA)

Voici un résumé de la méthode sous la forme graphique :

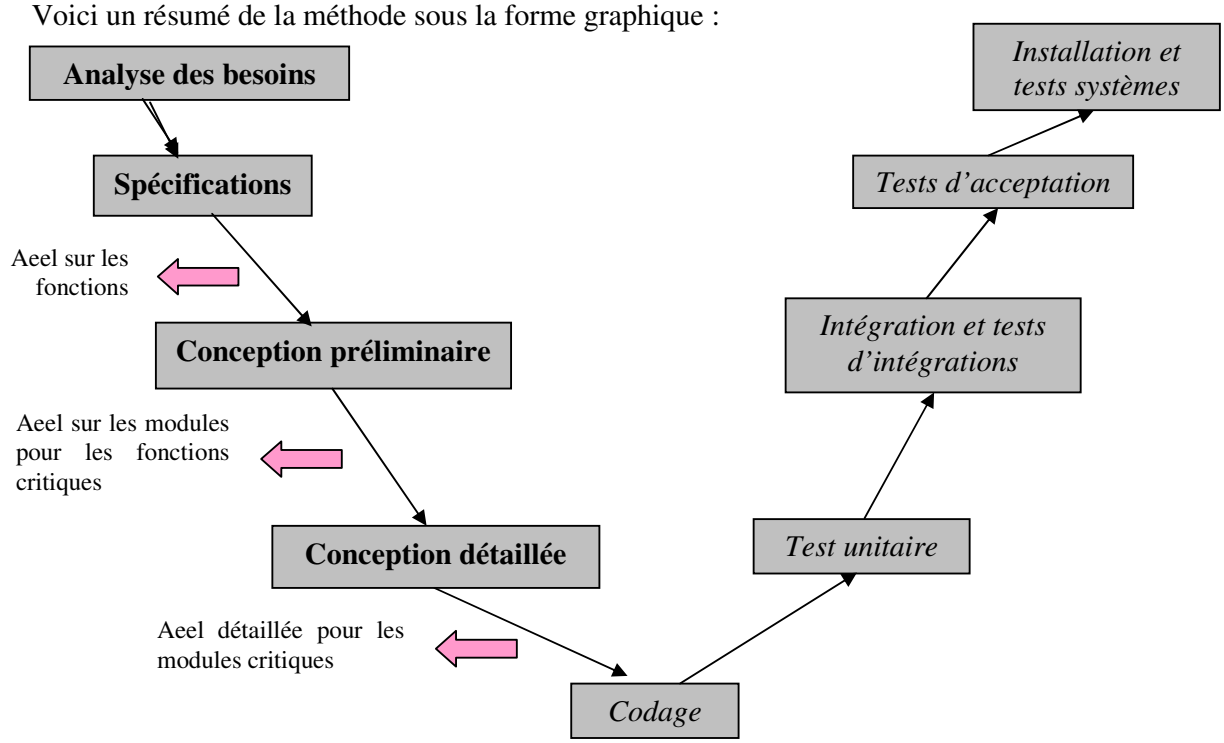


Figure 11 - Analyse des Effets des Erreurs sur le Logiciel (AEEL) [15]

3 Comment y remédier ?

Dans ce chapitre sont abordées les techniques d'amélioration (fiabilité et sécurité) et de développement logiciel pour remédier aux risques informatiques. Comme nous le verrons la démarche qualité est également un moyen de les réduire tout comme le plan de reprise d'activités.

3.1 Techniques d'amélioration de fiabilité

Il existe plusieurs techniques d'amélioration de la fiabilité. Dans ce chapitre, nous verrons les plus utilisés. Néanmoins, il y a un point commun entre toutes les techniques. Elles font des suppositions à propos des fautes potentielles afin de pouvoir couvrir l'ensemble de ces fautes.
Parmi ces suppositions, il y a la fréquence d'apparition des erreurs de transition de l'information.
Ce type d'erreur étant difficile à mesurer, nous y attacherons très peu d'importance.
Des exemples concrets de mise en place de la tolérance de panne seront également expliqués dans ce même chapitre (Paragraphe : *Traitement de la tolérance de panne dans FDDI* et paragraphe : *Les hypercubes*).

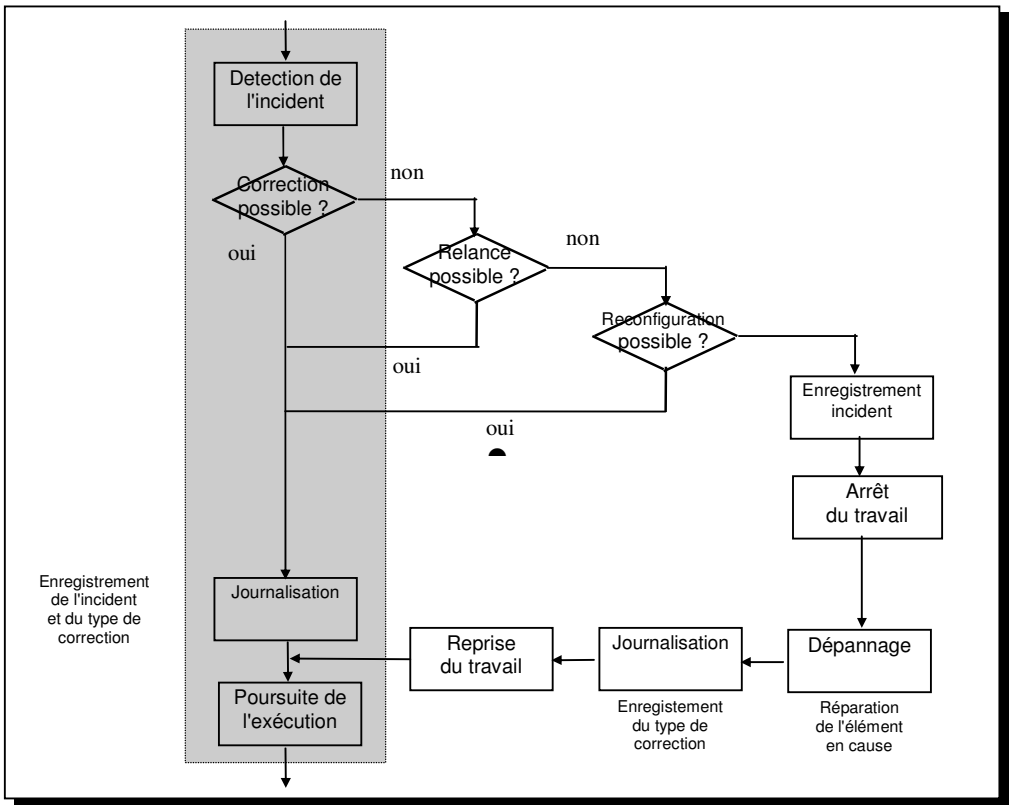
Tolérance aux pannes

Si l'on considère la chaîne « *faute* → *erreur* → *défaillance* → *pannes*[16] », la tolérance aux pannes regroupe les méthodes et techniques destinées à fournir un service conforme à la spécification en dépit des fautes[17].

[15] GEQC : Inspiré du cycle en V du *GEQC : Groupe d'Experts Qualité du CNAM*
[16] Définition du dictionnaire *Larousse* : « *Arrêt de fonctionnement accidentel et momentané* ».

Il s'agit de concevoir un système ne permettant pas à un sinistre de rendre inutilisable le système d'information.
Ce type de technique peut être mis en place au niveau matériel mais aussi au niveau logiciel.
Combinée avec d'autres, cette solution s'avère plus efficace pour minimiser les risques de pannes.

Principe de base de la tolérance de pannes



Explications
A la détection d'un incident matériel, un logiciel de surveillance prend en charge la panne.
Si la correction est possible, le traitement se poursuit alors.
Sinon le logiciel prend le relais et tente de relancer.
S'il y parvient, le traitement reprend (cas difficilement saisissable des *pannes fugitives*).
Sinon le logiciel recherche un *élément redondant* capable de poursuivre le traitement
S'il ne trouve pas ou que l'élément redondant est lui-même défaillant, la tâche en cours est interrompue complètement. Cette dernière reprendra son exécution après réparation.

Figure 12 - Principe de base de la tolérance de pannes

Le "Forward error recovery"

Cette technique demande à détecter une erreur et à se projeter dans le futur avec cette erreur pour essayer de prévoir les sinistres et trouver un palliatif rapide.
Cette technique utilise les principes de la redondance.
Ce procédé est utilisé dans les erreurs de communication, les gestions des erreurs mémoires, dans l'opérateur d'égalité des opérations arithmétiques.
La base de cette technique est la reconstruction de l'information en cas d'erreur.
Le prévisionnel va permettre de prendre des mesures alternatives en cas d'absence des ressources.
Les fautes peuvent parfois être masquées rendant difficile leur détection.
Dans ce cas, le résultat n'est pas émis tant que la correction de la faute n'est pas effectuée.

Le "Backward error recovery"

[17] 🕮 *Dependability : Basic Concepts and Terminology,* J.C LAPRIE, Dependable Computing and Fault-tolerant Systems, Volume 5, Springer-Verlag Wien New York, 1992, page 92.

Ici l'action est inversée par rapport au « *Forward error recovery* ». Lors de la découverte d'une erreur, la technique consiste à récupérer l'état du système « avant erreur », à relever les effets observés au moment de cette erreur ainsi que la propagation du sinistre résultant.
L'objectif étant de trouver une action alternative avant apparition de l'erreur.
Le problème ici est la reprise d'un état du système avec les données utilisateurs qui peuvent se trouver dans un état différent avant l'apparition de l'erreur et son apparition.
Cette solution plus sensible que les autres peut restituer un état du système cohérent, dégradé ou encore nécessiter l'arrêt complet du système faute de poursuite normale des traitements.

Codes correcteurs d'erreur

Le codage de l'information permet de détecter une ou plusieurs erreurs mais également de commuter sur l'organe redondant afin de poursuivre les traitements. Tout comme il existe plusieurs sortes d'erreurs, on rencontre également plusieurs types de codes :

- ***Code N/M, code itératif ou multiparitaire, code de Hamming.***

Bien entendu, il existe d'autres types de codage que nous n'étudierons pas ici[18].

3.2 Techniques d'amélioration de la sécurité

L'augmentation de la sécurité inclut également des techniques de logiciel.
Le plus important est d'éviter les différents types de vulnérabilité.
Le contrôle de la configuration de bout en bout est essentiel.
Le lancement du système doit être protégé des détournements de l'information qui pourraient être utilisées pour implanter des processus de type Cheval de Troie par exemple. Ces contrôles auront un impact sur l'intégrité du système d'information si aucune action adéquate n'est menée.
L'intégrité des données est de la responsabilité de la personne effectuant les saisies. De ce fait, les saisies doivent être enregistrées correctement.
L'authenticité est un critère important afin d'éviter des intrusions trop aisées dans le système d'information.
Il sera nécessaire de mettre en place des moyens d'identification, voire même des contrôles de signatures.
Tous ces mécanismes n'excluent pas le risque provenant des individus internes à l'entreprise.
Il est important de sensibiliser les utilisateurs du système d'information aux risques d'intrusion, aux risques encourus vis à vis de leurs données mais aussi en matière de sécurité informatique.
Les mots de passes fixes ne sont généralement pas recommandés si l'on souhaite sécuriser un minimum ses données.
Il en va de même sur la divulgation d'informations internes à l'entreprise.
La sécurité, oui, mais attention au caractère confidentiel des données; ceci est valable pour le personnel ayant accès à des informations confidentielles.
De plus le système d'information doit être protégé et disponible pour tous les moments où il doit être utilisé. D'où un taux de disponibilité conforme à l'utilisation.
La sécurité doit aussi minimiser la probabilité que le système soit accidentellement endommagé.
Afin de clore ce chapitre, il est important de noter la nécessité de tenir à jour la documentation du système d'information. Elle doit tenir compte de tous les aspects fonctionnels, mais aussi des palliatifs impératifs face à un événement nécessitant une action correctrice remédiant à un incident.

[18] ☞ Un chapitre est consacré à cette technique en annexe.

✓ ***Les techniques d'amélioration de la sécurité***[19] sont :

1. la décomposition modulaire — *segmentation d'un système en sous-systèmes multiples*
2. la composition modulaire — *agrégation de sous-systèmes entre eux en un système unique*
3. l'indépendance — *autonomie des sous-systèmes en place*
4. l'abstraction et l'encapsulation — *formatage d'un type de données orientées objets*
5. l'orientation objet — *manipulation d'une entité plutôt que d'un élément*
6. la paramétrisation — *fournir à un système les paramètres nécessaires à son fonctionnement*
7. l'héritage — *donner une propriété à la classe inférieure*
8. la localisation virtuelle — *localisation temporaire de données*
9. le réseau virtuel — *connexion temporaire entre deux systèmes*
10. la concurrence d'accès — *forme de contrôle d'accès simultané*
11. la réplication — *Duplication*
12. la restauration — *transition de service incorrect à service correct*
13. la tolérance de panne — *méthodes et techniques visant un service conforme à la spécification*
14. la cryptologie — *codage de données pour conserver la confidentialité de données*

Les techniques appropriées pour l'augmentation de la sécurité incluent une approche structurée : la *contribution principale* (symbole +), l'*implication d'un potentiel négatif* (symbole -) et la *contribution secondaire ou un effet potentiel* (symbole *[]*).

✓ Nota : Les données sécurisées incluent les notions de confidentialité et intégrité.

	Données sécurisées	Intégrité du système	Fiabilité, disponibilité du système	Identification authentification
Décomposition modulaire	+	+	+	[+]
Composition modulaire	[+]	[+]	[+]	+
Indépendance	+	+	+	+
Abstraction, encapsulation	+	+	+	+
Orientation objet	+	+	+	+
Paramétrisation	[+]	+	[+]	[+]
Héritage	+	+	+	+
Localisation virtuelle	+	+	+	+
Réseau virtuel	+	+	+	+ -
Concurrence d'accès	+	+	+	
Réplication	+	+	+	
Restauration	+	+	+	
Tolérance de panne	[+ -]	+	+	
Cryptologie	+			+

Tableau 13 - Techniques d'amélioration de la sécurité

Cryptologie et cryptographie

Longtemps synonymes, ces deux notions désignent pour la première la science des messages secrets et pour la seconde l'ensemble des méthodes mises en œuvres pour assurer ce secret[20].
De nos jours, de plus en plus d'informations doivent rester secrètes ou confidentielles. Par exemple, les banques ont un mot de passe qui ne doit pas être divulgué et que personne ne doit pouvoir déduire ou consulter.
Pour cela, nous avons recours à des mécanismes assurant la fonction de cryptage de l'information.

[19] 🕮 ***Computer Related Risks,*** Peter G. NEUMANN, édition : Addison Wesley, p 244.
[20] 🕮 ***La science du secret,*** Jacques STERN, édition Odile Jacob, 1997, page 10.

De nombreux mécanismes existent dont notamment DES[21] (massivement déployé par les banques pour garantir la sécurité et la confidentialité des données circulant sur le réseau bancaire) utilisé dans le système d'exploitation UNIX pour crypter les mots de passe.
Autre exemple, le commerce en ligne sur Internet nécessite aussi d'implémenter des logiciels de cryptage (problème des paiements sécurisés par cartes bancaires).
Pour effectuer cette fonction de cryptage, il faut mettre en place des méthodes.
De nos jours, les méthodes les plus courantes sont l'utilisation de clés privées ou clés secrètes, les clés publiques pour coder l'information avant cryptage.
Cette information codée sera cryptée par des algorithmes de type DES ou bien encore RSA[22], PGP[23] pour les plus connus d'entre eux.

3.3 Techniques de développement logiciel pour la sécurité informatique

Les techniques de développement logiciel permettent d'assurer la réponse aux besoins exprimés et explicites en termes de produits informatiques en augmentant la sécurité du système d'information.

Voici un certain nombre d'éléments contribuant à la sécurité des systèmes d'information dans le développement de logiciels. Ces techniques consistent à encapsuler des types de données abstraites mais également à autoriser et authentifier un utilisateur pour employer les services du système d'information et enfin à valider des entrées atomiques (synchrone à l'horloge atomique).

✓ ***Les techniques de développement logiciel*** intègrent en plus :

1. l'isolation stricte — *indépendance des sous-systèmes en place*
2. l'information cachée — *rendre privées des données pour une fonction logicielle précise*
3. le type sécurisé — *contrôle des actions possibles sur un type de donnée*

	Données sécurisées	Intégrité du Système	Fiabilité, Disponibilité du Système	Identification, authentification	Audit
Décomposition Modulaire	+	+	+	[+]	+
Composition modulaire	[+]	[+]	[+]	+	
Isolation stricte	+	+	+	+	+
Abstraction, encapsulation, Informations cachées	+	+	+	+	+
Type sécurisé	+	+	+	+	[+]
Orientation objet	+	+	+	+	+
Paramétrisation	[+]	+	[+]	[+]	[+]
Héritage	+	+	+	+	+
Localisation virtuelle	+	+	+	+	[+]
Réseau virtuel	+	+	+	+ -	[+ -]
Tolérance de panne	[+ -]	+	+		[+]

Tableau 14 - Techniques de développement logiciel

[21] DES : *Data Encryption Standard.*
[22] RSA : Initiales des trois auteurs de l'algorithme : Ronald RIVEST, Adi SHAMIR, Leonard ADLEMAN
[23] PGP : *Pretty Good Privacy* de Philip ZIMMERMANN.

Dans cette table, le signe + signifie qu'une contribution positive est apportée alors qu'un signe moins donne une contribution négative de la fonction spécifiée en fonction du type de sécurité.
D'une manière générale, un programme bien conçu et utilisant des techniques permettant de sécuriser un minimum le système d'information contribue à la sécurité de ce système ainsi qu'à l'intégrité des données en place.
Néanmoins ces techniques ne font qu'un minimum et ne sont pas suffisantes pour obtenir un niveau de sécurité optimal.
Ici nous nous limitons à la donnée proprement dite.
Ces techniques font l'objet d'arguments de vente au sein des entreprises conceptrices de logiciels spécialisés dans ce domaine et sont présentés comme la solution miracle apportée à la sécurité.
Bien entendu, cela n'est pas suffisant en règle général et demande des mécanismes complémentaires voire supplémentaires au sein du système d'information lui-même.

3.4 Exemples de réduction de risques informatiques

3.4.1 Traitement des pannes dans le réseau FDDI

Transmission

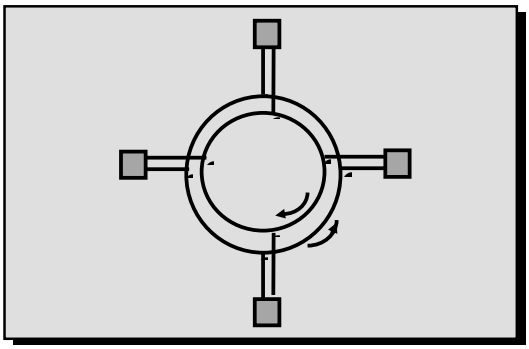
Chaque nœud a pour tâche de rétablir la transmission. S'il ne le peut pas un logiciel doit trouver une "*voie d'accès*" pour poursuivre le traitement. Le trafic est ainsi réorienté à travers des nœuds encore intacts. Il arrive que malgré tout, le logiciel échoue. Dans pareil cas, la panne est avérée. Notons là aussi l'existence d'un journal des erreurs et des types de corrections. Il fournit des statistiques sur l'état des transmissions du réseau pouvant servir à améliorer sa qualité.

Information

Généralement, les informations endommagées révèlent une trame altérée. Dans ce cas, un *code autocorrecteur* corrige l'information. Il arrive également qu'un simple renvoi de la trame suffise à effacer l'erreur.

FDDI

Le réseau FDDI[24] est un réseau en anneau à jeton à haut débit. En se basant sur deux boucles (en fibre optique) sur lesquelles les transmissions circulent en sens inverses, l'une par rapport à l'autre, FDDI est un bon exemple de réseau à tolérance de panne[25].



◆ ***Données chiffrées***
En théorie, avec FDDI le taux d'erreurs admissible est de l'ordre d'un seul bit erroné pour ($2,5 * 10^{10}$) bits transmis.

Comme le commente *Tannenbaum*, "la plupart des réalisations sont bien en deçà de cette limite.

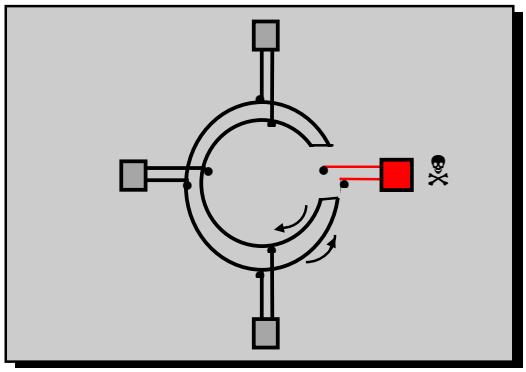
Figure 15 - Structure à double boucle du réseau FDDI

[24] FDDI : *Fiber Distributed Data Ïnterface*.
[25] *Réseaux*, André TANNENBAUM, édition : InterEdition, 3ème édition, 1997.

◆ **Traitement de la panne**

⇨ ***Première panne***

En cas de coupure de l'une des deux boucles, l'autre sert de système de secours. Derrière ce principe se cache l'idée de la *tolérance à la première panne*. En effet, de cette manière, une panne sur une des boucles, à cause d'une panne sur une station par exemple, n'interrompt pas le trafic des messages.



⇨ ***Deuxième panne***

Par contre, si la seconde boucle se rompt-elle aussi, les deux peuvent être reconfigurées pour n'en former qu'une seule. Ce principe permet une *tolérance à une seconde panne.*

↳ ***Performance***

Le parcours des trames est doublé. Les temps de transmission le sont également.

Figure 16 - Reconfiguration du réseau FDDI après coupure

La tolérance aux pannes influence les configurations des réseaux FDDI existants

Deux classes de stations ont ainsi été définies par la norme ANSI suivant le degré de tolérance aux pannes exigé.

⇨ **Stations de classe A**

Ces stations sont reliées aux deux boucles du réseau (comme sur les schémas ci-dessus). La tolérance aux pannes est maximale.

⇨ **Stations de classe B**

Par contre, ces stations ne se connectent qu'à une seule boucle. Évidemment, le coût est moindre mais le risque beaucoup plus important (il n'y a non seulement plus de tolérance à la seconde panne mais pas de tolérance non plus à la première).

De plus, dans le modèle OSI un certain nombre de correction d'erreur sont mis en place dans la couche 2 (couche liaison de donnée), que nous ne développerons pas ici.

3.4.2 Traitement des pannes par les hypercubes

Principe

L'hypercube est souvent utilisé dans les architectures multiprocesseurs à passage de messages bidirectionnels principalement pour la simplicité de leur routage. Un hypercube de dimension *n* se construit récursivement à partir d'un couple de nœuds. La numérotation des nœuds de ce couple se fait à l'aide d'un seul chiffre binaire : le premier nœud a le numéro 0 et le deuxième a le numéro 1. Ce couple est un hypercube de dimension 1. L'hypercube de dimension 2 est créé en numérotant à l'identique un autre couple et en joignant deux à deux les nœuds de même numéro. Chaque nœud reçoit donc ainsi deux chiffres dont le premier vaut 0 s'il appartient au premier hypercube, et 1 s'il appartient au second. Le second chiffre de chaque nœud garde la valeur du premier chiffre avant la jointure. Nous procédons de la même manière pour former un hypercube de dimension 3 en reliant deux hypercubes de dimension 2[26] (en reliant deux à deux les nœuds de numéro identique).

[26] 🕮 *Les ordinateurs massivement parallèles*, Cécile GERMAIN-RENAUD, Jean-Paul SANSONNET, Armand Colin, février 1991, page 53.

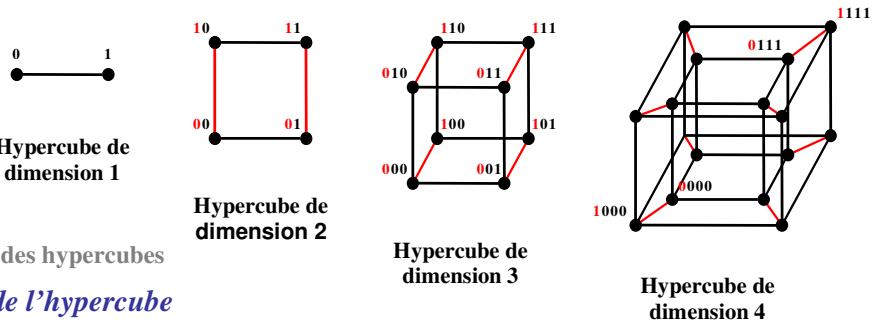


Figure 17 - La dimension des hypercubes

La tolérance de faute de l'hypercube

Un algorithme de routage s'appuyant sur la numérotation binaire est calculé pour l'hypercube. Cet algorithme est choisi en excluant tout interblocage. Si un nœud défaille, le chemin parcouru dans l'architecture de l'hypercube est remis en cause. Le moyen pour résoudre ce problème est de trouver un autre chemin dans l'arbre.

La tolérance de pannes se fait grâce à un algorithme particulier chargé de détecter les liens rompus. Chacun des nœuds analyse ses connexions aux nœuds suivants en envoyant un message de test à chacun d'eux. Ils doivent alors conserver l'état des liens aux nœuds voisins pour permettre la redirection des messages[27].

Sur la figure ci-jointe le nœud 011 a deux liens en erreurs.

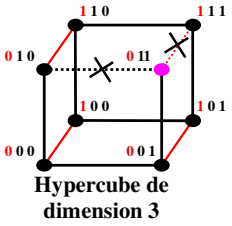


Figure 18 - Hypercube en erreur

3.5 Démarche qualité comme moyen de réduire les risques

Selon la norme ISO 8402, la qualité se définit comme un *ensemble de propriétés et caractéristiques d'un produit ou service qui lui confère l'aptitude à satisfaire des besoins exprimés ou implicites par rapport à des exigences de conformités*.

Il existe une relation entre les trois notions suivantes:

- la sécurité est un élément de la qualité, un produit non sûr et non fiable ne pouvant prétendre à un label de qualité respectable.
- la qualité, à l'inverse, fait partie de la sécurité, un système ne pouvant être sûr de fonctionnement si la qualité de ses éléments est mauvaise intrinsèquement.
- les performances d'un système comme d'une entreprise varient dans le même sens que la qualité de leurs produits et sont d'autant meilleures que leur fonctionnement n'est pas susceptible d'être taché d'insécurité.

La qualité d'un produit, d'un système ou d'un service est mesurée par son degré de conformité à ses spécifications, en supposant que les dites spécifications soient elles-mêmes conformes aux besoins exprimés par les commanditaires.

La qualité joue un rôle économique évident et prépondérant.

Un produit de haute qualité se vendra non seulement mieux mais les divers coûts de la non qualité seront minimisés le plus possibles engageant la confiance en ce dernier.

D'autre part, il est souvent moins coûteux de tolérer quelques erreurs résiduelles dans un logiciel que de passer au peigne fin les programmes, instruction après instruction, pour diminuer le taux d'erreurs existantes.

La question est de savoir si une erreur oubliée ne risque pas, dans un certain contexte particulier, d'avoir des conséquences graves et néfastes pour tout le système.

Par opposition à la non qualité courante, une faille de sécurité entraîne un sinistre ressenti comme une rupture par rapport à un état antérieur de stabilité de fonctionnement.

Nous pouvons citer les catastrophes naturelles, les accidents, les concours de circonstances, les erreurs ou les malveillances.

[27] 🕮 *A fault-tolerant Tree communication scheme for hypercube systems*, Y-R LEU, S-Y KUO, IEEE transactions on Computers, volume 45, juin 1996, pages 645-651.

La sécurité dans cette approche est la gestion des accidents prévisibles mais également imprévisibles.
La question que nous pouvons nous poser est de savoir si nous pouvons nous limiter, dans l'analyse des risques de l'entreprise, aux failles de sécurité, sans nous préoccuper des aspects liés à la qualité.
Si les problèmes liés à la qualité sont pris en compte, nous pouvons nous demander où et quand nous pouvons et devons nous arrêter : qualité du personnel, qualité des cahiers des charges, qualité des spécifications, du choix des matériels et des techniques de programmation, qualité des bâtiments, qualité de l'organisation, qualité du management, etc.
Nous risquons donc de remettre en cause toute la structure et l'organisation de l'entreprise dans le cadre d'une analyse des risques des systèmes d'information trop fine.
En réalité, tous ces éléments concourent effectivement à la plus ou moins grande sécurité des systèmes d'information et de l'entreprise elle-même.
A quel moment l'inexactitude- caractère incomplet, non-qualité d'une donnée - est elle une faille d'intégrité ?
Dans la pratique, nous nous limiterons souvent à la détermination de problèmes potentiels de non-qualité identifiable. Les conséquences concrètes dans le déclenchement d'un sinistre doivent être connues , surtout si elles sont potentiellement graves.
L'exemple typique est celui du logiciel intervenant dans les processus critiques et dont nous ne pouvons faire l'économie de l'analyse de la qualité.

3.6 Plan de reprise d'activités

Le plan de reprise d'activités signifie qu'il y a déjà une panne constatée. Il va consister à remettre le système d'information en état fonctionnel normal, supprimer les traces de dommages causés et restaurer la disponibilité et l'exactitude des informations préalablement existantes.
Dans un plan de reprise d'activités, il faut distinguer trois types de plan qui ne sont surtout pas à négliger :

- **Plan de sauvegarde**
- **Plan de « backup »**
- **Plan de continuité d'activité** utilisateur

Le but recherché est de minimiser les pertes d'informations.

3.6.1 Elimination de la vulnérabilité

Dès qu'une vulnérabilité est mise en évidence, son élimination doit être entreprise systématiquement.
Ne pas engager une action corrective fait montre de négligence.
La cause exacte d'une vulnérabilité n'est généralement pas connue.
Il est de la responsabilité du fabriquant ou du vendeur de fournir les actions correctives pour pallier les vulnérabilités du système analysé.
Cela peut s'avérer très long et dans ce cas il faut envisager d'autres palliatifs plus adaptés et plus efficaces.
Nous allons voir plusieurs méthodes pouvant être considérées pour lutter contre la vulnérabilité d'un système d'information.

Application d'un correctif
Un correctif, plus communément appelé « patch », est un petit logiciel permettant de contrecarrer une vulnérabilité pour une application donnée. L'avantage de ce procédé est sa rapidité de développement, de mise en œuvre et de déploiement sur site.

Son désavantage est qu'un même problème sur une autre application fera l'objet d'un autre développement.
Un « patch » est destiné par rapport à une vulnérabilité et une seule application.

Désactivation d'un service
Désactiver un service transportant une vulnérabilité permet d'éviter l'exploitation malveillante de cette vulnérabilité.
Si le service impacté n'est pas très sollicité, l'impact au sein de l'entreprise sera par voie de conséquence minimisé.

Nouvelle conception
Revoir la conception d'une application s'avère être une opération coûteuse mais aussi la plus sûre à long terme au niveau sécurité.
En effet, la sécurité doit être implémentée à l'origine de la conception elle-même et non pas être un module rapporté.
En adoptant ce principe il en résultera une augmentation de la sécurité du système d'information.

3.6.2 Amélioration de la protection

Le fait d'apporter une amélioration voire un renforcement de la protection sous-entend qu'il y a déjà en place une protection d'un niveau inacceptable pour les besoins présents.

Nous distinguons deux modes de protections :
- la *révision* des protections
- la *création* de nouvelles protections

Révision des protections
Nous allons améliorer ici l'ajustement et la révision des procédures de protection par rapport à une nouvelle vulnérabilité constatée.

La création de nouvelles protections
Dans ce cas, nous allons nous intéresser à l'analyse portée sur la protection d'un sous système d'information.
Le but est de savoir s'il est nécessaire d'avoir une protection sur tel ou tel service, de créer des protections là où elle était absente si une fois mise en évidence par l'apparition d'un incident elle démontre que ce service, partie ou sous partie du système d'information, était sensible.

3.6.3 Mise à jour de la détection

Lorsqu'une vulnérabilité est exploitée et les protections contournées, le dernier recourt pour minimiser les risques est la détection d'un incident.

Modifications de configuration
Dans ce type de mise à jour, nous devons passer en revue les vulnérabilités connues et voir si des modifications aux systèmes de détection d'intrusions pourraient les prendre en compte. A cette occasion il peut être possible de revoir les méthodes d'alerte ainsi que la liste des personnes devant être prévenues en pareil cas.

Moyens de détection supplémentaires

L'analyse du système de protection doit permettre de savoir si de nouveaux mécanismes de détections seraient justifiés pour améliorer la rapidité de détection.
Cette opération doit être réalisée régulièrement pour maintenir à jour les moyens de détection.

3.6.4 Restauration des données

Avant de réaliser une restauration des données, il est nécessaire de connaître la cause du problème et d'y remédier.
C'est la qualité des informations utilisées pour la restauration qui détermine la qualité du système restauré.
Il faudra aussi s'assurer au préalable de la validité des informations à restaurer.
Généralement dans une entreprise, le système d'information peut présenter des défaillances mais ce n'est pas pour autant que les utilisateurs ne travaillent pas correctement.
Cela pose le problème des mises à jours des données. A-t-on les dernières modifications enregistrées ?
Afin de traiter correctement ce sujet, il faut distinguer plusieurs notions :

- La *disponibilité*
- L'*intégrité*
- La *confidentialité*

La disponibilité
Si l'on dispose d'une sauvegarde sûre (dernier état du système d'information), c'est le moyen le plus rapide pour restituer au plus un maximum de disponibilité du système d'information. Sinon, il faudra reconstituer les données en effectuant les traitements nécessaires pour remettre le système dans un état fonctionnel avec les dernières sauvegardes de données utilisateurs.
La mise à jour des sauvegardes doit se faire régulièrement afin de minimiser les pertes de données.

L'intégrité
Dans la majorité des cas, il faudra restituer les données à l'aide de la dernière sauvegarde sûre. Si les données ont été modifiées et non détruites, il peut être difficile de localiser les parties altérées. La vérification des données peut être un travail long et fastidieux.

La confidentialité
Si le système d'information a été altéré, il y a de fortes chances pour que la confidentialité soit compromis.
Le seul remède est d'évaluer l'étendue de la compromission et stopper la diffusion.
Il peut être envisagé de prendre des mesures réactives pour limiter l'impact de la compromission.

D'une manière générale, il faut s'assurer de l'intégrité des données restaurées avant de procéder à la restauration des services associés.

3.6.5 Restauration des services

Tout comme la restauration des données, la restauration des services associés va subir le même découpage.

La disponibilité
Pour certaines entreprises, la disponibilité est plus importante que la restauration des données (chez les fournisseur de services INTERNET par exemple).
Ce facteur primerait sur la sécurité pour les entreprises ayant besoin d'un taux de disponibilité important.
Néanmoins un problème subsiste.
Restaurer un service avant de restaurer le système et avoir vérifié le bon fonctionnement de celui-ci sans résidu d'incident, peut faire l'objet de réapparition d'attaques. Il peut devenir vite difficile de maîtriser d'éventuels intrus (hacker).Si toutefois cette opération s'avère obligatoire, il est plus judicieux d'effectuer une sauvegarde complète du système afin de rechercher ultérieurement la cause de l'incident.
Ce type de manipulation peut présenter un danger dans le cadre des réseaux d'entreprises.

L'intégrité
La restauration de l'intégrité des données nécessite de s'assurer au préalable d'avoir vérifié l'ensemble des constituants du système d'information.
Les attaques externes compromettent souvent l'intégrité des services en mettant en place du code malveillant (exemple: Cheval de Troie).

La confidentialité
Dans le cas d'attaques externes par un hacker par exemple, il est fréquent que la confidentialité des données soit rompue par un petit logiciel lui permettant d'acquérir les informations qui l'intéressent sans compromettre les données déjà existantes.
Le système d'information doit alors être suffisamment sécurisé pour éviter de redémarrer avec un système dégradé.

3.6.6 Acteurs de la confiance restaurée

Un plan des incidents de sécurité s'avère utile afin de pouvoir préparer une communication constructive sur les incidents .
Il faut pouvoir montrer aux différents membres de l'entreprise que nous sommes restés maîtres de la situation afin de préserver et restituer le système d'information de l'entreprise.
Pour cela, il faut qu'une certaine confiance s'installe entre le responsable du système d'information et les employés de l'entreprise.

La direction
La direction va allouer un budget pour améliorer la sécurité du système d'information.
Elle doit être convaincue de la nécessité de l'investissement face aux sinistres qu'elle pourrait rencontrer si aucune action n'est menée pour améliorer la sécurité des données, convaincue aussi des résultats techniques et financiers pou l'entreprise par soucis de préserver les intérêts de cette dernière.
Elle doit donc avoir confiance en son département informatique en matière de sécurité et apprécier la capacité de ce service à maîtriser les incidents.

Les actionnaires
Ce sont eux les propriétaires de l'entreprise.
Ils ont donc besoin de connaître et de comprendre l'impact financier de tout incident de sécurité.
Les actionnaires doivent être convaincus que leurs intérêts ont toujours été protégés et que toutes les mesures ont été prises rapidement et efficacement.

Les utilisateurs
Ils sont directement impactés par les arrêts du système d'information et de la sécurité de leurs données. C'est leur travail qui est interrompu voire détruit.
Les utilisateurs ont besoin d'être rassurés sur la restauration de leurs données, l'intégrité de leur données.
Si les utilisateurs n'ont plus confiance en leur département informatique, ils vont essayer de remédier à leurs différents problèmes par eux-mêmes.
Cette dernière possibilité serait assez conséquente en terme de coût, poserait des problèmes de traitement de l'information, serait lourde à gérer et laisserait l'utilisateur libre de sa sécurité, ce qui pourrait avoir un impact négatif sur l'ensemble du système d'information.
Là aussi, il est très important que les utilisateurs puissent se décharger de ces tâches fastidieuses et puissent les remettre à un service compétent en qui ils peuvent avoir confiance tant sur la confidentialité des données que dans l'intégrité et la sécurité de leurs données.

Les partenaires
Le partenariat s'appuie sur un climat de confiance mutuelle entre les entreprises.
Si toutefois cette notion est altérée après un incident de sécurité, les relations de partenariat risquent d'être menacées elles aussi.
Les partenaires doivent avoir en retour la confiance qu'ils ont eue en l'entreprise ne serait-ce que par la conviction de la protection effective de leurs données. Ils doivent être rassurés sur les possibles attaques externes à travers leurs propres partenaires.

Le public
Le public doit avoir confiance non seulement dans la qualité mais aussi dans les responsabilités de l'entreprise.
Il doit être convaincu que l'entreprise est capable de faire face à n'importe quelle situation de crise.
Il doit avoir la certitude que l'entreprise met tout en œuvre pour le bien du public.

4 Conclusion

La problématique soulevée par ce document probatoire montre la nécessité de la prise en considération du *risque informatique*.
Nous avons vu au travers de ces différents chapitres des méthodes et techniques permettant de remédier ou minimiser le risque informatique autrement dit le taux de vulnérabilité d'un système d'information donné. Nous avons abordé pour y répondre et y remédier plusieurs *concepts*, *outils*, *méthodes* associés à des *exemples*.

Le risque est une notion à ne surtout pas négliger. Les paramètres à prendre en compte pour l'analyse des risques sont la *fiabilité*, la *sécurité*, la *maintenabilité* et la *disponibilité*. Nous avons également constaté que la *divulgation* d'information joue un rôle important et qu'il devient nécessaire de sensibiliser de plus en plus le personnel de l'entreprise contre ce type de négligences coupables.

De même, il est important de se doter de moyens techniques efficients pour faire barrage ou rendre plus difficiles les attaques externes au système d'information. Cette mise en œuvre a un *coût financier* non négligeable qu'il faut prendre en compte dès le départ lors de la mise en place de tout plan de sécurité.

Plus la vulnérabilité est prise en charge tôt dans la réalisation, moindres sont les coûts ultérieurs engendrés par un éventuel sinistre. C'est pourquoi nous avons étudié des *méthodes de mesure des risques* telles que EBIOS, FEROS, MARION et MEHARI permettant d'apprécier un risque et d'amener une solution pour pallier un sinistre éventuel avant qu'il n'apparaisse et endommage le système.

D'autre part, nous avons vu que l'analyse porte sur un jugement et une appréciation d'un risque par la personne qui réalise cette analyse. Néanmoins, il ne faut pas tomber dans l'extrême et mettre en place des mécanismes trop contraignants quand nous savons pertinemment qu'un sinistre particulier n'arrivera pas ou a peu de chances de se produire. Plus les mécanismes sont lourds à gérer, à mettre en œuvre et à maintenir, plus l'investissement de l'entreprise sera important et sera difficile à budgéter. A l'inverse, il ne faut pas implémenter une configuration minimale et se dire que les risques sont minimes compte tenu du niveau de sécurité physique de l'entreprise. Par voie de conséquence, cela reviendrait à minimiser le niveau de protection optimale.

Dans le dernier chapitre, il a été traité du problème de reprise d'activités après l'apparition d'un sinistre. En effet, un plan de reprise d'activités n'est utilisé qu'uniquement après la survenue d'un sinistre parfois dévastateur.
L'intégrité des données pour la reprise des services est fondamentale.
Des questions impératives doivent être posées, telles que : tous les risques ont-ils été envisagés ? Notre système d'information a-t-il un niveau de protection optimale contre la vulnérabilité : accidents, erreurs et malveillances ? Peut-il être remis en service sans générer d'autres sinistres ? et enfin concrètement : Possédons-nous de façon certaine et disponible la dernière mise à jour de nos données ?

En règle générale, force est de constater que les entreprises investissent trop peu dans ces techniques et malheureusement souvent trop tard. La gestion du risque après dommages devient plus délicate. Il faut en pareil cas et en premier lieu en éradiquer la cause pour éviter la diffusion ou la création de nouvelles vulnérabilités du système.

L'essentiel est de mettre en place un mécanisme de protection correspondant au niveau de sécurité souhaité, en fonction de la criticité des informations de l'entreprise, tout en alertant toutes les parties sur les risques perçus par les différentes analyses effectuées, sans omettre la responsabilisation et la formation des utilisateurs du système d'information.

De nos jours, nous sommes de plus en plus nombreux à manipuler d'importantes données informatiques, encore faut-il les préserver de toute détérioration et éviter toute utilisation pouvant être néfaste, voire désastreuse, pour l'entreprise toute entière dont la survie peut en dépendre.

5 Table des illustrations

6 Lexique

AEEL
Analyse des Effets des Erreurs sur le Logiciel

APSAD
Assemblée Plénière des Sociétés d'Assurances Dommages

Attaque logique
Utilisation non autorisée de ressources du système d'information, conduisant à un préjudice au moins qualitatif pour la victime, se traduisant essentiellement par une perte d'intégrité et/ou de disponibilité, entraînant souvent un profit indirect pour le criminel et/ou le commanditaire éventuel.

Bombe logique
Programme restant à l'état inactif tant qu'il n'est pas réveillé par un événement système (souvent une date).

Cheval de Troie
C'est un programme apparemment innocent qui contient des instructions cachées. Lorsqu'il est lancé, ce sont ces instructions qui s'exécutent et accomplissent sans difficulté leurs méfaits.

CLUSIF
Club de la Sécurité des Systèmes d'Information Français.

CRAMM
CCTA Risk Analysis and Management Methodology:

DES
Data Encryption Standard

Divulgation
C'est l'utilisation non autorisée des ressources du système d'information, entraînant la divulgation à des tiers d'informations confidentielles.

Fraude
Utilisation non autorisée de ressources du système d'information, conduisant à un préjudice évaluable monétairement par la victime, essentiellement formé de détournement de biens au profit du criminel.

ISDF
Institut de la Sûreté de Fonctionnement

GEQC
Groupe d'Experts Qualité du Cnam

MEHARI
Méthode Harmonisée d'Analyse du Risque Informatique)

Parasites
C'est une séquence d'instructions ajoutée à un programme destinée à extraire des informations à partir de ce programme.

PGP
Pretty Good Privacy de Philip Zimmermann

RSA
Ronald Rivest, Adi Shamir et Leonard Adleman

SNIFFER
Programme épiant les informations circulant dans un système à la recherche d'un type d'information.

Spoof
Personne ou programme prenant l'identité d'une autre entité de même nature soit pour masquer sa propre identité, soit pour convaincre sa victime de lui accorder des services auxquels elle n'aurait normalement pas accès.

Ver
Programme utilisé en mécanisme de transport pour d'autres programmes. Il utilise le réseau pour se propager de machine en machine. Il exploite un point faible du réseau (courrier électronique, remote access par exemple).

Virus
Programme infectant un autre en se dupliquant dans ce programme.

7 Bibliographie

A fault-tolerant Tree communication scheme for hypercube systems
Y-R LEU, S-Y KUO, IEEE transactions on Computers, volume 45, juin 1996.

Computer Related Risks
Peter G. NEUMANN, édition : Addison Wesley.

Dependability : Basic Concepts and Terminology
J.C LAPRIE, Dependable Computing and Fault-tolerant Systems, Volume 5, Springer-Verlag Wien New York, 1992.

La science du secret
Jacques STERN, edition : Odile Jacob, 1998.

Le risque informatique : modélisation, évaluation, réduction (épuisé)
Jean-Philippe JOUAS; Albert HARARI; Jean-Marc LAMERE; Jacques TOURLY, édition d'organisation, 1992.

Le Trésor, dictionnaire des sciences
Michel SERRES et Nayla FAROUKI, édition Flammarion, 1997.

Les ordinateurs massivement parallèles,
Cécile GERMAIN-RENAUD, Jean-Paul SANSONNET, Armand Colin, février 1991.

Etude d'un modèle de performances de matrices redondantes de disques
Mémoire d'ingénieur Cnam, Jean-Jacques CHANDEZ, 1998.

Présentation de l'Aeel
Denis CHAUVIN, Skaubine LOISEL, dirigée par Alexis TODOSKOFF, Institut des Sciences et Techniques de l'Ingénieurs d'Angers (ISTIA), 2001.

Réseaux
André TANNENBAUM, édition : InterEdition, 3ème édition, 1997.

Sécurité des systèmes d'information
Donald L. PIPKIN, édition : Campus Press, 2000.

Serveurs multiprocesseurs clusters et architectures parallèles
René CHEVANCE, édition : Eyrolle, 2000.

8 Internet

Cryptologie
http://www.multimania.com/marief

Etudes et statistiques sur la sinistralité informatique en France Année 2000 - CLUSIF
http://www.clusif.asso.fr

Méthodologie
http://www.securite-informatique.com
http://perso.wanadoo.fr/2si.mehari.htm

Réseau : Fiber Distributed Data Interface (FDDI)
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/fddi.htm

9 Annexes

9.1 Codes correcteurs d'erreurs simples

Le codage de l'information permet de détecter une ou plusieurs erreurs mais également de commuter sur l'organe redondant afin de poursuivre les traitements. Tout comme il existe plusieurs sortes d'erreurs, on rencontre également plusieurs types de codes :

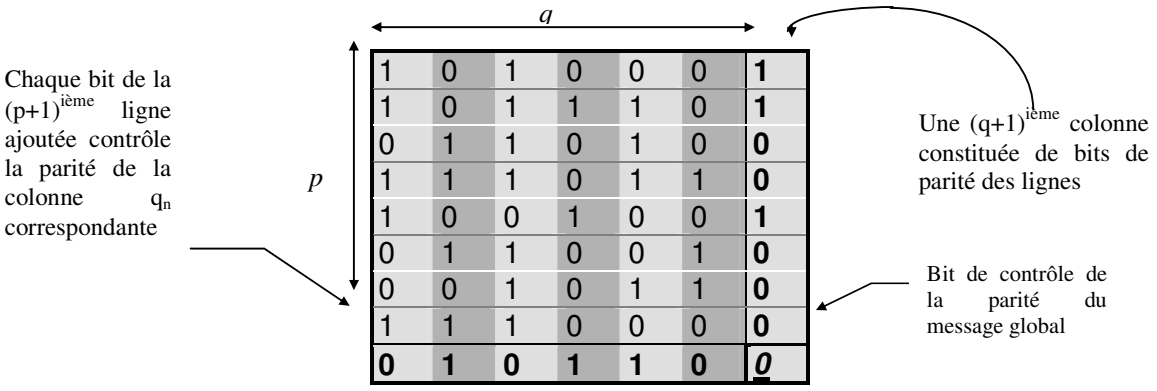
- ***Code N/M, code itératif ou multiparitaire, code de Hamming***.

9.1.1 Code N/M

Chaque caractère est représenté à l'aide de M bits dont N sont égaux à 1 et M-N égaux à 0. On utilise la position des N bits à 1 dans le mot pour distinguer les caractères entre eux. Le contrôle d'un mot s'effectue en comptant les bits à 1.
Le code N/M n'est pas optimal surtout dans la correction des erreurs.

9.1.2 Codage itératif ou multiparitaire

Les informations *n* sont écrites dans une grille rectangulaire de dimension {*p*,*q*} où *p* représente les lignes et *q* les colonnes.



1	0	1	0	0	0	**1**
1	0	1	1	1	0	**1**
0	1	1	0	1	0	**0**
1	1	1	0	1	1	**0**
1	0	0	1	0	0	**1**
0	1	1	0	0	1	**0**
0	0	1	0	1	1	**0**
1	1	1	0	0	0	**0**
0	**1**	**0**	**1**	**1**	**0**	***0***

ici p = 9, q = 7 et n = 48

Tableau 19 - Codage itératif ou multiparitaire

9.1.3 Code de Hamming

Fréquemment utilisé dans l'industrie, nous retrouvons ce type de codage partout où il y a duplication d'une information. Leurs constructions sont simples : parmi tous les mots d'une longueur donnée de *n* digits, on choisit ceux qui diffèrent entre eux par la valeur de *d* digits au moins.
Nous nous limitons ici à donner les grandes lignes de cette technique. Elle est basée sur la Distance de Hamming - calcul du nombre de bit différent entre deux mots binaires.
La distance de Hamming **D** peut être calculée de la façon suivante :

$D = 2^{e+1}$ où **e** est le *nombre d'erreurs*

Si les mots binaires reçus ont un bit en erreur et dont l'état a changé de 0 à 1 ou de 1 à 0. (distance de Hamming de 2)
La gestion devient difficile lors de l'apparition d'erreur dans les deux mots binaires à comparer. Cette technique s'avère être peu efficace dans le cas d'erreurs massives ou de coupure d'un des sous systèmes.
Dans le cas d'apparition fréquentes de ces erreurs dans l'environnement du système d'information, nous aurons recours à d'autres techniques plus efficaces.

Exemple

Soit l'ensemble des mots de 4 digits, leur nombre diffère entre eux par la valeur d'un seul digit. Il est donc de 16. Un code de Hamming peut être défini en choisissant tous les mots différant par deux digits au moins.

Ici, nous avons choisi le premier arbitrairement puis placé les mots suivants dans un ordre quelconque (les mots ne satisfaisant pas au critère, et par conséquent rejetés, ne figurent pas dans les listes).

Code de Hamming sur mots de 4

1010	0000
1100	0011
1111	0101
0000	0110
0011	1001
0101	1010
0110	1100
1001	1111

Tableau 20 - Code de Hamming sur mot de 4

Forme du code de Hamming

Les codes de Hamming sont généralement constitués de 2 parties :

- une première composée d'un nombre binaire naturel (ici les trois digits les plus à gauche dans notre second exemple),
- une seconde comportant un certain nombre de bits de codage dépendant de la distance de Hamming *d* choisie. Ces bits de codage, dits de parité, portent chacun sur un groupe déterminé de bits situés plus à gauche. Dans notre exemple, le bit de parité des trois autres est à droite.

Distance de Hamming

Un ensemble de mots de longueur donnée a des valeurs arbitraires *d* appelées *distance de Hamming*. Sa constitution s'effectue grâce à une méthode matricielle.
Le degré de protection de l'information dépend de la valeur du code de Hamming.

L'emploi

Les avantages du code de Hamming résident donc dans son efficacité dans la protection des données mais également dans son faible encombrement.
Il est surtout utilisé dans les mémoires E.C.C. (« Error Correcting Code » = Code auto-correcteur de mémoire) et également dans les réseaux.

Caractéristiques	H	A	M	M	I	N	G	Calculs
Distance de Hamming *d*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	**d**
Nombre d'erreurs détectées à 100%	*0*	*1*	*2*	*3*	*4*	*5*	*6*	**d-1**
Nombre d'erreurs indép. Corrigées	**0**	**0**	**1**	**1**	**2**	**2**	**3**	**(d-1)/2 si d impair d/2-1 si d pair**

Tableau 21 - Distance de Hamming

Nombre d'erreurs corrigées par le code de Hamming

Nombre de bits d'information disponibles	Nombre	de bits	à ajouter	pour le	codage
1	1	2	3	4	5
2	1	3	4	6	
3 – 4	1	3	4		
5 - *8* – 11	*1*	*4*	*5*		
12 – 26	1	5	6		
27 – 31	1	5	7		
M	*1*	*p*	*p+1*		

Tableau 22 - Correction par le code de Hamming

RESUME

Le risque informatique est un sujet souvent négligé bien qu'il montre une obsession de sécurité résultant d'une juste appréhension. Dans ce domaine pourtant de nombreuses solutions très efficaces ont vu le jour ces dernières années. Ce document probatoire vise à les présenter pour expliquer le moyen de ***remédier aux risques informatiques***.

MOTS-CLES

Risque, fiabilité, vulnérabilité, sécurité, maintenabilité, disponibilité, tolérance de panne, méthodes.

ABSTRACT

The informatical risk is very often disregarded although it shows a fear which expresses an obsession resulting of a justified apprehension. Nevertheless, in that field, many efficient available solutions appeared these last few years. This probatory document aims at developping the way to ***find solutions in front of the informatical risks problems***.

KEY-WORDS

Risk, fiability, vulnerability, security, maintenability, disponibility, fault tolerance, methods.