Judicaël GROS-DESIRS Gilles JOSPITRE Fouad EL-HARMOUZIA Xavier MATHIS

Projet sécurité

MEthode Harmonisée d'Analyse de RIsques

Sommaire

INTRODUCTION 3

1. MEHARI : Qu'est ce que c'est ? 4
1) Définition 4
2) Historique 4
3) Principe de fonctionnement 5

2. Mise en place de la méthode 6
1) Plan stratégique 7
2) Plan opérationnel de sécurité 8
3) Plan opérationnel d'entreprise 9

3. Développement de MEHARI 13
1) Recherche des informations pour la mise en place de la méthode 13
a) Vue générale de l'entreprise 13
b) Test technique de l'infrastructure réseau 16
2) Synthèse des données récoltées 17
3) Analyse et application de la méthode 17
4) Les Logiciels mettant en place Méhari 20

4. Autres méthodes de gestion des risques 22

5. Actualités 23
1) Politique de gestion des risques en France 23
2) Autres moyens de gestion des risques 23

CONCLUSION 25

ANNEXE 26

INTRODUCTION

Généralités

La réalisation de ce projet rentre dans le cadre de notre formation IUP. Dans la matière « sécurité » on s'intéresse aux différents d'aspects de la sécurité dans les réseaux informatiques présents au sein des entreprises.

Nous avons une équipe de quatre éléments pour nous partager les travaux de recherches, de synthèses et mise en pratique de la méthode chez RDI.

Sujet du projet

Le but de ce projet est de travailler sur la méthode MEHARI. Cette méthode consiste à une gestion des risques au niveau d'une entreprises. On travaille sur plusieurs niveaux que l'on détaillera au fur et à mesure de notre exposé.

1. MEHARI : Qu'est ce que c'est ?

Avant tout il est important de définir de quel sujet on va parler. On va présenter le rôle de la méthode et son historique.

1) Définition

La méthode Méhari résulte des travaux de Jean-Philippe Jouas et de Albert Harari, alors chez Bull (le premier Directeur de la sécurité du Groupe, le second responsable des méthodes au sein de cette Direction) et de leur consolidation au sein de la commission Méthodes du Clusif (Club de la Sécurité des Systèmes d'Information Français).
Albert Harari avait développé Melisa pour la DCN (Direction des Constructions Navales de la Délégation Générale pour l'Armement) et cette méthode proposait une certaine vision des risques, avec des paramètres d'évaluation relativement simples et adaptés à la cible visée. Son utilisation dans un contexte industriel et dans un Groupe international a conduit Jean-Philippe Jouas et Albert Harari à faire évoluer cette base pour définir un modèle du risque complet et une métrique associée.
Les résultats de ces travaux ont été publiés en 1992 (Le Risque Informatique - Editions d'Organisation).
Les éléments fondateurs contenus dans cet ouvrage se sont révélés stables et ont peu évolués depuis. Une mise à jour récente du document d'origine est disponible sur ce site dans la partie Bibliothèque (Le Risque Informatique).

Reprise par le CLUSIF et permet une analyse et une évaluation quantitative des facteurs de risques à chaque situation difficile que pourrait rencontrée l'entreprise. Elle permet de concilier les objectifs stratégiques et les modes de fonctionnements de l'entreprise. La nouveauté de cette méthode est qu'elle prend en compte les derniers modes de fonctionnement de l'entreprise avec une politique de gestion des risques à un bon niveau.

2) Historique

Méhari existe en Français et en Anglais et est maintenue par le CLUSIF. Elle est dérivée des méthodes Marion et Mélisa (qui eux n'évoluent plus depuis plusieurs années). Méhari est utilisée par de nombreuses structures publiques et privées en France mais également au Québec.

3) Principe de fonctionnement

La méthode méhari prend avant tout en compte les informations de l'entreprise afin de développer un plan afin de mieux définir les points à protéger dans l'entreprise.
MEHARI permettra à l'entreprise de définir :
- Un plan stratégique de sécurité
- Un plan opérationnel de sécurité par site ou entité
- Un plan opérationnel d'entreprise
- Le traitement d'une famille de scénarios ou d'un scénario particulier
- Le traitement d'un risque spécifique (Accident, Erreur, Malveillance)
- Le traitement d'un critère de sécurité (Disponibilité, Intégrité, Confidentialité)
- Une application critique supportant le business
- Un projet critique (infrastructure, application…)

La méthode MEHARI, quant à elle, conjugue la rigueur d'une analyse des risques liés formellement au niveau de vulnérabilité du système d'information, à l'adaptabilité de la gravité des risques étudiés. En effet, la présence ou l'absence de mesures de sécurité va réduire ou non, soit la potentialité de survenance d'un sinistre, soit son impact. L'interaction de ces types de mesures concoure à réduire la gravité du risque jusqu'au niveau choisi.

Le modèle de risque MEHARI se base sur :
- Six facteurs de risque indépendants : trois influant sur la potentialité du risque et trois influant sur son impact ;
- Six types de mesures de sécurité, chacun agissant sur un des facteurs de risque (structurelle, dissuasive, préventive et de protection, palliative et de récupération).

Les phases de **MEHARI** sont les suivantes :

- ✓ Phase 1 : établissement d'un plan stratégique de sécurité (global) qui fournit notamment :
  - la définition des métriques des risques et la fixation des objectifs de sécurité,
  - la reconnaissance et la détermination des valeurs de l'entreprise,
  - l'établissement d'une politique de sécurité entreprise, l'établissement d'une charte de management.
- ✓ Phase 2 : établissement de plans opérationnels de sécurité réalisés par les différentes unités de l'entreprise

- ✓ Phase 3 : consolidation des plans opérationnels (global).

Nous allons détailler ces différentes étapes dans la suite de notre rapport, en étudier les modalités et les moyens à mettre en œuvre.

2. Mise en place de la méthode

Méhari répond aux besoins des entreprises dans la gestion des risques et la mise en place des solutions des risques. Ce n'est pas une méthode d'audit. Il s'organise autour d'axes principaux qui résument les données essentielles au bon fonctionnement d'une entreprise.
La méthode MEHARI (MEthodes Harmonisée d'Analyse de RIsques) est avant tout une méthode d'analyse et de management de risques. Elle a été conçue pour être adaptable au contexte de l'entreprise mais elle ne dispose pas de déclinaison par typologie d'entreprise ou métier.

MEHARI se présente comme un ensemble cohérent d'outils et de méthodes de management de la sécurité, fondés sur l'analyse des risques. Les deux aspects fondamentaux de MEHARI sont le modèle de risque (qualitatif et quantitatif) et les modèles de management de la sécurité basés sur l'analyse de risque. MEHARI vise à donner des outils et des méthodes pour sélectionner les mesures de sécurité les plus pertinentes pour une entreprise donnée.

Méhari se nourrit des enjeux et des objectifs de l'entreprise afin de livrer un résultat « business » quant aux mesures de sécurité à mettre en œuvre. Les différentes phases sont d'établir le contexte d'entreprise, d'identifier les actifs et les menaces, d'analyser les risques et enfin de définir les mesures de sécurité (traitement du risque).

La méthode Méhari a été conçue pour les grandes entreprises et organismes (qui sont également les principaux demandeurs de méthodologie de risques) et prévoit la démarche de sécurité de l'information à deux niveaux :

_Niveau stratégique : niveau liée au métier de l'entreprise et indépendantes des processus et technologies mise en œuvre. Ce niveau fixe les objectifs de sécurité et le métrique des risques.

_Niveau opérationnel : entité, filiale, branche, business unit qui met en œuvre cette politique et la décline en analyse précise des risques, définition des mesures de sécurité à mettre en œuvre et pilotage de la sécurité dans le temps (contrôle et tableau de bord).

1) Plan stratégique

C'est le plan qui examinera l'entreprise sur un aspect général. Ici on parle d'une façon ou d'une autre du business. Serons pris en compte lors de cette analyse, la classification des ressources de l'entreprise, l'ensemble des risques existants, ses objectifs sécurité.

Première étape mettre en avant les risques possibles :

Lors de l'audit nous allons donc répertorier les risques pouvant pénaliser l'activité de l'entreprise cliente.
Ensuite pour chacun des risques détectés on définit :

- Son potentiel :

C'est-à-dire la capacité de destruction. C'est pour cela que l'on mettra en place des tests ou plus précisément des scénarios qui permettent de se mettre en situation et dévaluer ce potentiel.

-Son impact :

En clair, une fois la catastrophe arrivée concrètement quel seront les dégâts réels.

-Sa gravité :

Déterminer si vraiment les dégâts son handicapants pour l'entreprise et son fonctionnement.

Deuxième étape limite d'acceptabilité :

De part ces caractéristiques nous allons ensuite mettre en place une échelle pour le degré d'acceptabilité non seulement sur le plan de la gravité mais aussi du temps. Combien de temps l'entreprise pourra être dans cette handicape sans que cela devienne dangereux pour ça survie.

Troisième étape les ressources de l'entreprise :

Lors de cette étape nous définirons en fait les valeurs de l'entreprise, quels services génèrent le plus de chiffre d'affaire, ou sont vital pour le fonctionnement de la société.

Quatrième étape solution et indicateurs :

C'est l'étape finale, c'est lors de celle-ci que l'on mettra en place dans un premier temps les indicateurs afin de prévenir au maximum l'arrivée d'une catastrophe. que l'on regroupera toutes les informations que l'on a pu récupérer et qu'on les analysera de façon globale afin de pouvoir mettre en œuvre des solutions : règles de sécurité et de responsabilité. Les solutions s'applique sur plusieurs niveaux :
Ce découpage permet un regroupement des mesures en six grandes familles :

— Les **mesures structurelles** qui jouent sur la structure même du système d'information, pour éviter certaines agressions ou en limiter la gravité.

— Les **mesures dissuasives** qui permettent, dans le cas d'agresseurs humains, d'éviter qu'ils mettent à exécution la menace potentielle en déclenchant l'agression.

— Les **mesures préventives** : celles qui permettent d'empêcher les détériorations ou d'éviter qu'une agression n'atteigne des ressources du système d'information.

— Les **mesures de protection** qui, sans empêcher les détériorations, permettent tout au moins d'en limiter l'ampleur.

— Les **mesures palliatives** qui agissent une fois les détériorations accomplies, et qui permettent, d'une part d'en limiter les conséquences au niveau de l'entreprise, d'autre part de restaurer les ressources détériorées pour retrouver l'état initial.

— Les **mesures de récupération** qui visent à récupérer une partie du préjudice subi par *transfert des pertes sur des tiers*, par le biais des *assurances* ou de dommages et intérêts consécutifs à des *actions en justice*, dans le cas d'agresseurs humains.

2) Plan opérationnel de sécurité

- Spécifier le domaine et les outils : élaboration des scénarios.

Périmètre et niveau de détail Elaboration des scénarios Validation de la classification

- Auditer le niveau de sécurité : audit des services

Audit des services et sous services Consolidation au niveau cellules

- Evaluer la gravité des scénarios : Potentialité/ Impact/ Gravité

Détermination Potentialité/Impact/gravité

- Exprimer les besoins de sécurité : mesures générales et spécifiques

- Planifier les actions de sécurité : mesures prioritaires

Mesures spécifiques et prioritaires Autres mesures hiérarchisées

3) Plan opérationnel d'entreprise

Dans cette étape il s'agit fondamentalement de mettre en place des scénarii sur les impacts et les conséquences que peuvent avoir ces sinistres sur la vie et le bon fonctionnement de l'entreprise. Cette partie conclue la boucle de l'application de la méthode Méhari par la mise en place d'un outil permettant le suivi des opérations à effectuer afin d'améliorer la sécurité de la société.

- En effet, on va choisir en fonction des analyses des informations récoltées ci dessus, différents types de risques auxquels l'entreprise étudiée risque de s'exposer. Ce ci permet alors d'établir une éventuel couverture de ce genre de risque.
- L'élaboration des indicateurs consiste à déterminer les niveaux de gravité que peut supporter une entreprise en fonction des risques encourus. On se penchera bien sur plus sur les risques majeurs ayant le plus d'impact sur le fonctionnement de l'entreprise
- Viens alors le moment d'effecteur un bilan de toutes les informations collectées. Il est essentiel d'établir des corrélations entre les différents acteurs de cette étude. Une synthèse doit être faîte afin de dessiner au mieux les contours d'une action que ce soit au niveau de l'entreprise, de la gestion des scénarii et des nouvelles consignes communiquées aux salariés.

Pour que cette stratégie soit couronnée de succès il est nécessaire de s'assurer que :

- ✓ Elle est connue et comprise par la Direction et le personnel de l'entreprise

- ✓ Elle est pilotée et sa mise en œuvre est assurée et mesurée
- ✓ Elle reste pertinente dans le temps
- ✓ Elle se décline en objectifs stratégiques reliés à des objectifs tactiques (ensemble des initiatives, projets, processus et organisation) qui forment un tout cohérent et contribuent pleinement à l'atteinte de la couverture des risques
- ✓ Elle est financée et que les budgets sont affectés avec l'assurance de leur meilleure contribution au succès de cette stratégie

C'est à ce niveau qu'intervient la mise en place et le suivi d'un Tableau de Bord Equilibré Sécurité (TBES). En effet, la démarche TBES mise au point par HAPSIS s'inspire des principes de gouvernance des systèmes d'information et de la mise en œuvre de « Balanced Score Cards ». Elle intègre l'ensemble des rapports de cause à effet entre les paramètres clés, les mesures de résultats et les boucles de suivi pour la mise en œuvre de la stratégie. En outre, la démarche TBES est **pragmatique**, **modulaire** et s'applique de préférence périmètre par périmètre.

Bénéfices :

- ✓ Les objectifs poursuivis par la stratégie sécurité sont conformes à ceux de l'entreprise

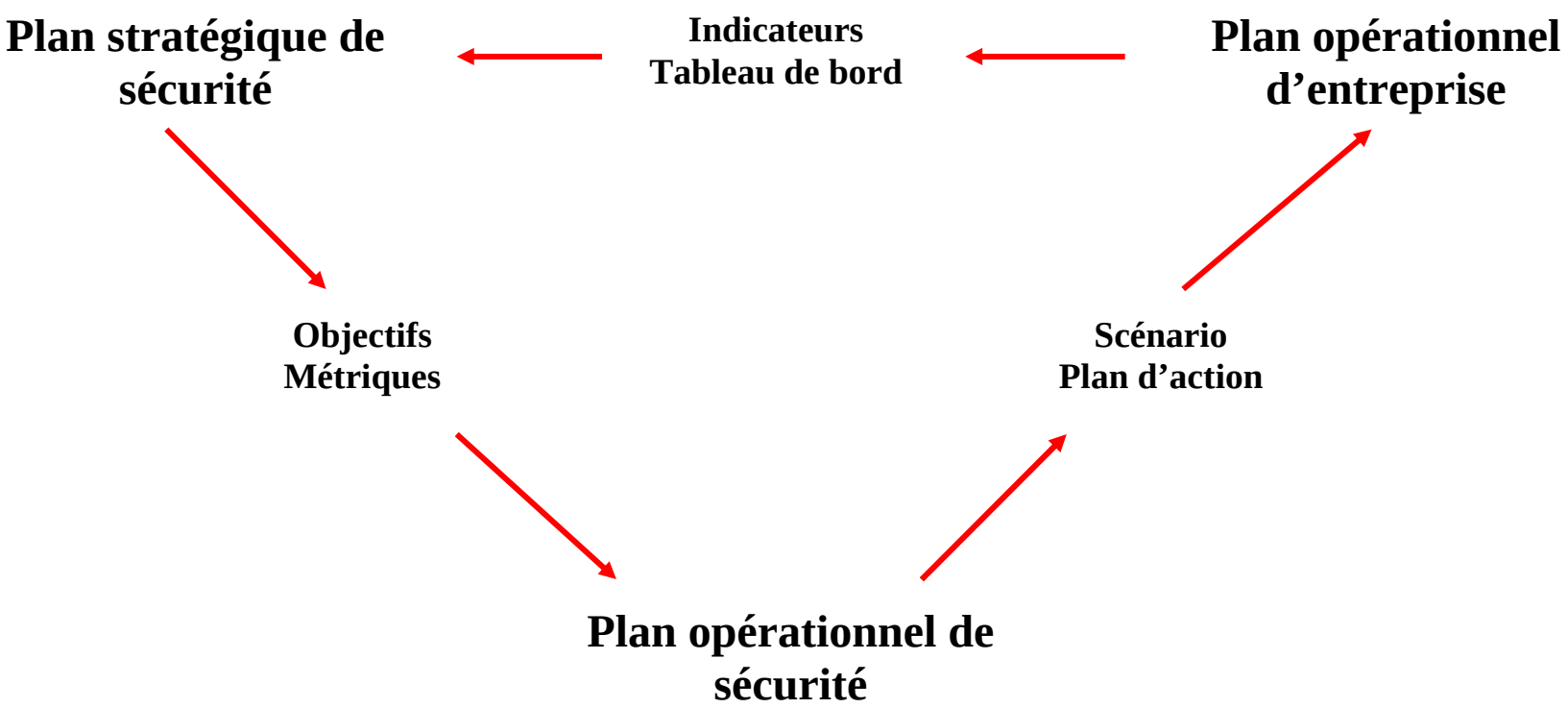
Valorisation accrue de l'action menée par le RSSI qui est ainsi replacée au sein de la stratégie de l'entreprise

- ✓ Impact sur l'image véhiculée par la SSI
- ✓ Pilotage et mesure dans la durée de la stratégie sécurité sur l'ensemble de ses aspects, en privilégiant le caractère stratège du RSSI
- ✓ Intégration des aspects stratégiques et opérationnels

Arbitrage budgétaire avec l'assurance du meilleur impact sur le niveau de sécurité.

La mise en pratique d'un TBES permet de disposer d'un outil de pilotage de sa stratégie sécurité ainsi que de conduite du changement. Clarifiant, communiquant et explicitant la stratégie de sécurité, il provoque une adhésion du personnel et optimise l'affectation des moyens. De ce point de vue, les probabilités de succès de la stratégie de sécurité sont améliorées. Cela se traduit par une atteinte des objectifs sur les indicateurs de risques et se matérialise par une diminution des évènements de pertes propres aux risques considérés.

La démarche MEHARI



3. Développement de MEHARI

Afin d'illustrer au mieux notre exposé nous avons décidé de mettre en place une petite simulation de la méthode auprès d'une entreprise. Par hasard notre choix s'est porté sur la société RDI basé à NIMES.

1) Recherche des informations pour la mise en place de la méthode

Comme vu précédemment on constate que une bonne partie des informations de la méthode méhari doit être cherchée au sein de l'entreprise. Pour cela nous avons en trois rendez-vous avec M. Fleury récolter les données nécessaires à l'application de la méthode.

a) Vue générale de l'entreprise

La première étape fut de récolter des information très générales sur le fonctionnement de l'entreprise. Puis de déterminer les niveaux d'acceptabilité des risques inventoriés. Puis on peut mettre en place l'architecture de la méthode méhari, de l'analyse des données jusqu'à la simulation de scénarii catastrophe.

Entreprise :

- 1ere étage : 400 m² et 2rez de chaussez 600 m²
- SSII (chaque société du Groupe est spécialiste d'un métier)
- 3 sociétés qui forment le groupe RDI
- Effectif : 80 personnes

SOCIETES	ACTIVITE
RDI	- **Couverture des besoins d'infrastructures** : matériel, réseau, communication inter-sites, sécurité, contrat d'assurance...
Novécom méditerranée	- **Réponse aux besoins de stratégie collaborative :** intranet, portails d'entreprise, gestion de la connaissance, applications web ...
ICE Informatique	- **Réponse aux besoins de gestion d'entreprise :** comptabilité, paie, états financiers, gestion commerciale, suivi relation client ...

Personnel :

- Les équipes sont motivés et adhèrent complètement aux objectifs de l'entreprise

- Climat social OK
- Pas de protection contractuelle des données
- Dans le règlement intérieur pas de clause de confidentialité
- L'entreprise ne pense avoir des données secrètes à protéger par contrat
- Accès aux procédures est protégées mais pas drastiquement
- Pas d'audit externe concernant le contrôle des procédures et les contrôles d'accès
- Une équipe pour la gestion des stocks
- Bonne situation dans l'entreprise même si le secteur reste morose
- Services de proximité
- Homogénéité de la clientèle 50% de nouveaux clients
- Investissement important de la société
- Rachat de quelques sociétés dans le sud de la France

Le groupe RDI semble assez incontournable dans son secteur d'activité sur la région

Inventaire des risques et limite d'acceptabilité

Eléments les plus importants	Risques	Limite d'acceptabilité
Messagerie (dépannage à	Ecroulement du serveur	½ journée de coupure
ERP (facturation et devis)	Panne ou dysfonctionnement du service	1 journée
Salle d'hébergement	Problème du à l'humidité inondation	1 journée
Stock	Incendie Inondation Vol	

Sécurité générale dans l'entreprise

Protection contre les incendies

Extincteurs disposés dans toutes les pièces. Des trappes de désenfumages sont également disposées dans différentes pièces. Un plan de l'entreprise est également placé à l'entrée et à l'étage. Tout est mis en œuvre pour faciliter une éventuelle intervention des pompiers.

Contrôle des va et vient dans l'entreprise :

- ✓ tous les salariés ont un badge magnétique pour entrer et sortir de l'entreprise

- ✓ Seulement 5,6 personnes ont un accès total à l'informatique (salle des serveurs, …)
- ✓ Pas de badge pour les visiteurs

Accès à la salle des serveurs ?
La porte est verrouillée, l'accès est limité à 5,6 personnes et de réalise avec leurs badge
Est-ce que le personnel se délogue ou verrouille leur station lorsqu'il quitte leur poste ?
non, sauf le soir ->FAILLE

Protection de l'intégrité des informations :

La gestion des sauvegardes :
quotidienne pour l'ensemble des serveurs dans une baie de disque
hebdomadaire (effectué chaque week end) sur bande. (RDI tourne sur 10 bandes gardé à l'extérieur).
A chaque modification : sauvegarde Ghost
Sécurité des disques : raid 5 (sur les serveurs et sur la baie de disques)

Il y a un responsable pour les sauvegardes.
Il n'existe aucune procédure pour effectuer ces sauvegardes.

En cas de plantage
système de restauration sur disque à partir du serveur de sauvegarde

Protections logicielles et antivirus
Logiciels : un antivirus est installé sur chaque station et sur la messagerie
Mise à jour automatique pour les sauvegardes

Comment se passe les connexions de RDI au client ?
Soit par VPN (sécurisé)
Soit par RDP (logiciel de prise de main à distance -> pas sécurisé)

Comment est gérée la gestion des journaux d'erreurs, des logs, analyses, des performances réseaux et systèmes ?
les erreurs sont gérées à partir d'un logiciel de supervision

Les assurances

Il y a une responsable administrative et financière qui s'occupe du bon fonctionnement et du renouvellement des contrats d'assurances.

AOM, coutier mondial (assurance Groupama)

Le contrat souscrit inclus :
Véhicule (accident de la route, …)
Multirisque <=> le mobilier et locaux (vol, incendie, catastrophe naturelle, …)
Responsabilité civile (dommage commis aux tiers)

Il n'est pas inclus :
certaines catastrophe naturelle (tronc d'arbre, …..)
divulgation d'information

Remarque : les assurance sont assez frileuses pour assurer les SSII, surtout celles qui travaillent au niveau conseil / audit / sécurité

b) Test technique de l'infrastructure réseau

Pour la partie concernant les tests techniques, M. FLEURY nous a indiqué une liste de logiciels qu'on pourrait tester dans les locaux de l'entreprise.

Lannetscan

C'est un logiciel permettant d'effectuer un scanner de son réseaux afin de détecter les vulnérabilités présentes ce dit réseau étudié. Il propose en outre quelques solutions pour remédier à ces failles.

NetworkView3

Netsniffer

C'est un logiciel intéressant quand il s'agit de l'étude d'un réseau local. Il permet par exemple de tester si les postes de travail reçoivent bien ou transmettent bien des données. Il permet aussi à une machine d'analyser en temps réel les données qu'elle émet. Ce qui permet en outre de savoir si une machine n'envoie pas de données sans l'autorisation de l'utilisateur. Ce logiciel est aussi capable de récupérer des trames au plus bas niveau du réseau. Il permet une lecture rapide les informations essentielles comme l'adresse des émetteurs et récepteurs ainsi que les protocoles utilisés.

SnifMon 3.10.103

C'est un logiciel qui sert lui aussi à faire une analyse du réseau. Il effectue une capture puis permet une analyse des trames mais cette fois ci en temps réel. Il supporte les protocoles IP, TCP, UDP et d'autres encore.

Tenable NeWT

Ce logiciel est sûrement le plus utile de tous dans le type de travail qu'il nous ait demandé dans le cadre de l'implémentation de la méthode MEHARI. En effet, il s'agit d'une plate forme idéale pour les consultants en sécurité dans la mise en place d'audit.
Tenable n'est autre qu'un scanner de vulnérabilité d'un réseau donné. C'est l'adaptation du logiciel Nessus pour les plates formes WINDOWS.
Ce logiciel peut être aussi utilisé par les entreprises possédant des serveurs WINDOWS afin d'effecteur des contrôle sur la solidité de leurs réseaux locales. D'ailleurs on peut noter que ce logiciel permet la mise en place d'un mode distribué pour nourrir toutes les machines de son réseau des ressources de cet outil.
Ce logiciel est très complet, permet la mise en œuvre de nombreuses sources de vulnérabilités en proposant aussi les solutions qui lui semblent les plus appropriées pour résoudre des détails.
Il repère des failles aussi variées que : des problèmes de configurations sur des serveurs mails, ftp ou web, l'ouverture des ports sur les machines, les services P2P ou autre services suspicieux, repérage de virus etc.…
Ce logiciel est aussi compatible sur les machines Linux et Unix.

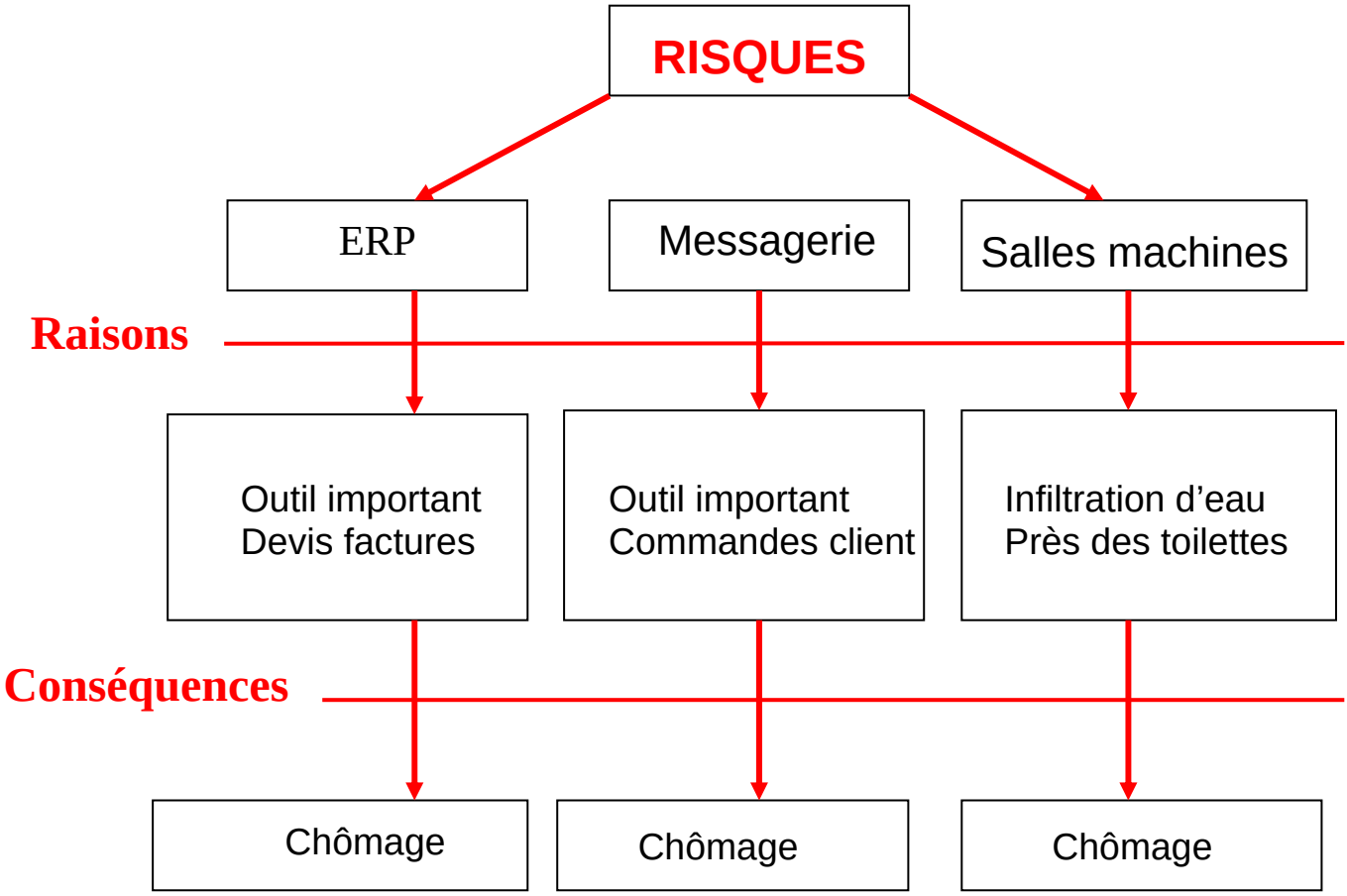
Le résultat de ces tests sont disponibles en annexe

2) Synthèse des données récoltées

La synthèse des données a simplement consisté à la lecture des données et la mise en forme des ses information afin de tenter de scénariser une catastrophe.

3) Analyse et application de la méthode

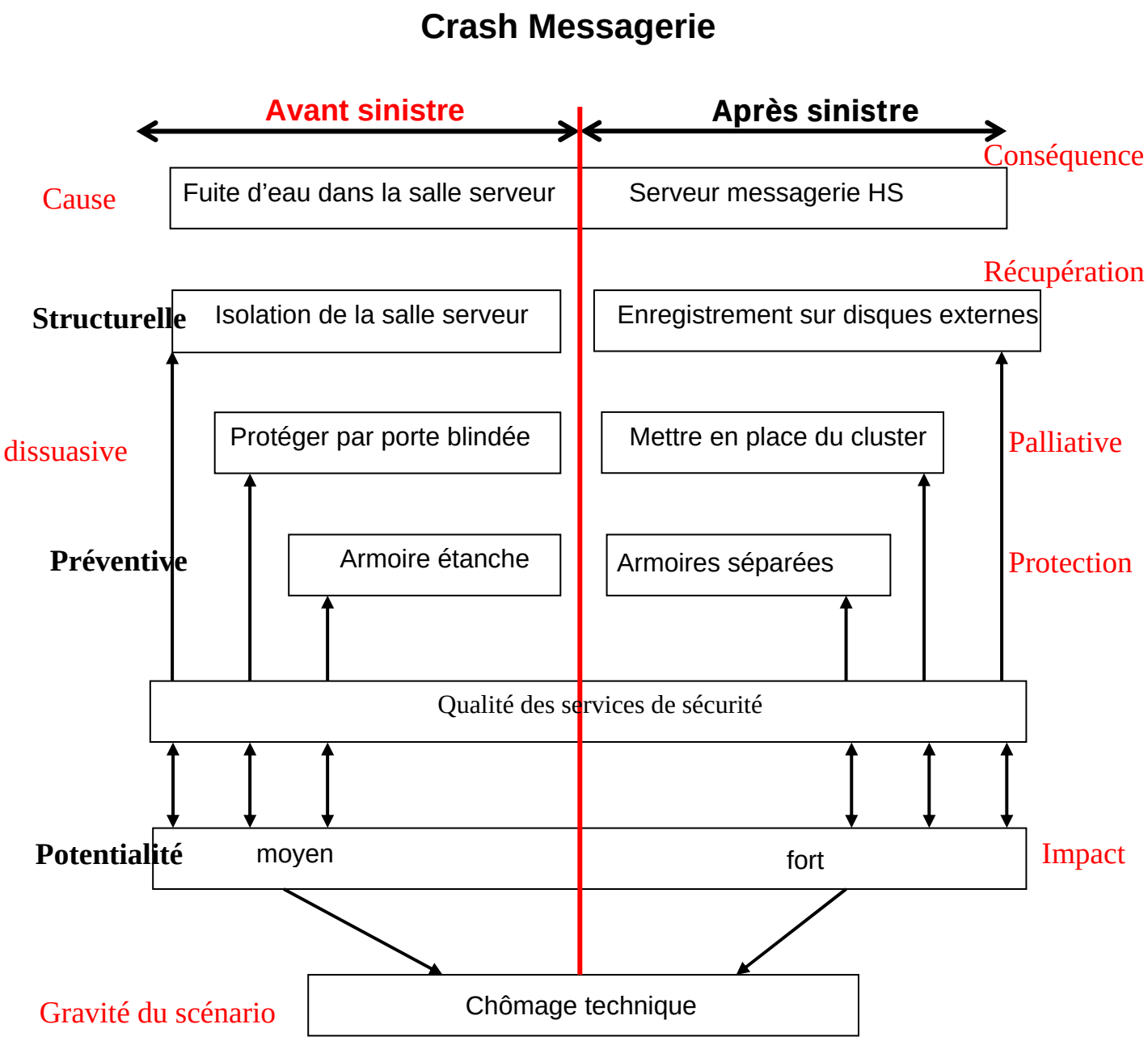
Après avoir fait l'analyse de toutes ces données, nous nous sommes attachés à sélectionner quelques scénarii catastrophe, les conséquences, les causes, les impacts et le plus important les données à prendre en compte afin de solutionner ces problèmes.


RISQUES
ERP
Messagerie
Salles machines
Raisons
Outil important
Devis factures
Outil important
Commandes client
Infiltration d'eau
Près des toilettes
Conséquences
Chômage
Chômage
Chômage

Les scénarios mis en place pour RDI :

A partir du plan stratégique de sécurité nous allons donc pouvoir mettre en place une série de scénarios possibles pour ces risques. Nous appliqueront un scénario a deux des trois risques répertoriés.

Pour la messagerie :



Au vue de ce scénarios on peut se rendre compte des actions entraîné par le risque du crash de la messagerie de l'entreprise. On peut aussi voir de façon plus explicite les différentes mesure a prendre dans le cadre de la mise en place d'un plan sécurité. Le même schéma sera donc mis en place pour tous les risques répertorier d'une entreprise cliente.

4) Les Logiciels mettant en place Méhari

Risicare

Risicare vous permet de réaliser une analyse de risques liée à un 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. 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 étudiée. 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 gravite à partir de l'audit précédemment réalisé. Risicare, par des codes couleurs associes, permet de voir immédiatement quelles sont les failles de sécurité les plus significatives et leur localisation.

- La construction d'un plan d'action visant à réduire la gravite des scénarios de sinistres les plus critiques. Cette phase peut être vue comme une véritable simulation d'actions a entreprendre, Risicare donnant immédiatement leur influence sur la gravité des scénarios de sinistres.

L'ergonomie de Risicare, son installation simplifiée et une aide en ligne comportant de nombreuses rubriques méthodologiques et techniques facilitent grandement la réalisation d'une analyse. Celle-ci sera conduite par le client final qui pourra utilement (en fonction de son niveau de connaissances de la méthode MEHARI) se faire assister d'un spécialiste).

La société qui met en place ce logiciel est BUC SA

Edition de logiciels d'analyse de risques

Conseil en management et en organisation de la sécurité :
- Audits généraux de sécurité, et analyse de risque MEHARI
-Audits spécialisés de sécurité (tests d'intrusion, audits applicatifs, etc.)
- Fournisseur de produits logiciels méthodologiques

Editeur de logiciels : RisicareConception d'outils propriétaires d'analyse de risques sécurité des réseaux

Créée en 1987, BUC S.A. en est aujourd'hui à sa troisième génération de progiciels d'analyse de risques. Les produits écrits par BUC S.A. sont ainsi présents dans 150 grands comptes en Europe, Afrique, Canada et Amérique Latine.BUC S.A. consacre d'importants moyens en recherche et développement qui ont permis la sortie du progiciel Risicare s'appuyant sur la méthode MEHARI et en assurent l'évolutivité. Parallèlement à la production de ces outils standards, plusieurs développements spécifiques sur la gestion des risques ont été réalisés dans les domaines bancaire, de la santé et de la grande distribution.

Progiciel d'analyse de risques RISICARE.RISICARE utilise le modèle de risques développé par la méthode MEHARI, sa simplicité d'emploi rend les concepts de la méthode facilement assimilables. La version 3 apporte de nouvelles fonctions quant à la production de tableaux de bord orientés "Risques" (suivi de la gravité d'un ensemble de scénarios). La personnalisation des bases de connaissances (questions d'audit et scénarios) est facilitée par l'import - export vers des tableurs. L'ouverture du produit permet notamment de traiter des risques spécifiques (liés aux réseaux, à l'internet, à l'e-commerce, etc.…)Assistance et formation dans la mise en place de RISICARE.Etude et conception d'outils propriétaires d'analyse de risques.

SCORE

SCORE™ est un logiciel qui se situe par rapport à l'ensemble des domaines de sécurité définis dans la méthode MEHARI™ développée par le CLUSIF.
SCORE™ permet également de mesurer les efforts restant à fournir pour se mettre en conformité avec les exigences définis par les différentes entités métiers de l'entreprise (extrait d'une analyse des enjeux).

Les modules inclus dans le logiciel SCORE™ version MEHARI™ sont les suivants :
Module 1 : Organisation de la sécurité et aspects juridiques
Module 2 : Sécurité des bâtiments, des locaux et de l'environnement de travail de l'utilisateur
Module 3 : Sécurité des réseaux, des télécoms et de leur exploitation
Module 4 : Sécurité de la production informatique
Module 5 : Sécurité des systèmes et leur architecture
Module 6 : Sécurité des applications et des développements applicatifs
En fonction des points faibles identifiés, des analyses avec des outils complémentaires sont alors envisageables.

SCORE™ est un outil performant d'auto évaluation, totalement personnalisable et adaptable à la politique de sécurité de l'entreprise.
Son utilisation très simple permet de rapidement se situer par rapport à la norme ISO/IEC 17799:2000, aujourd'hui reconnue et très largement utilisée par de très nombreuses entreprises.
SCORE™ permet également de mesurer les efforts restant à fournir pour se mettre en conformité avec la politique de sécurité définie en interne et basée sur cette norme.
Les modules inclus dans le logiciel SCORE™ sont les suivants :
Questionnaire ISO/ IEC 17799:2000
Définition de la stratégie de sécurité
Mesure de la conformité

4. Autres méthodes de gestion des risques

La méthode EBIOS qui a pour objectif de déterminer les actions de sécurité, les expressions de sécurité. Elle fait une étude des risques et identifie les objectifs de sécurité.

La méthode MARION permet de déterminer :

_des scénarios d'incidents.
_leur impact sur la disponibilité, l'intégrité ou la confidentialité.
_leur gravité sur une échelle de 4 niveaux
_les scénarios classés selon leur gravité
_des mesures de réduction des risques

MARION établit une notation sur la base d'un questionnaire est fait une évaluation par rapport à une norme, repérage des failles importantes.

La méthode MELISA qui analyse des enjeux (menaces, risques, coût), de vulnérabilité (étude existant) et propose des parades (plan d'action) et permet d'établir un suivi.

5. Actualités

1) Politique de gestion des risques en France

Vu le travail que nous avons effectué il nous semble alors évident de mettre en place une politique de sécurité solide. Même si Méhari est le nouveau must en matière de politique de sécurité en France il se trouve que peu d'entreprises effectue ce travail sur leurs installations. Pourtant force est de constater que les coûts entrepris dans ce genre d'opération ne sont en rien comparables à ce que pourraient coûter des dégâts sur les infrastructures essentielles au fonctionnement d'une société.
Selon une enquête du CLUSIF, plus de 85% des entreprises françaises envisagent de mener des actions de sensibilisation de leur personnel à la sécurité informatique.
Difficile néanmoins d'envisager une formation classique mobilisant chaque personne pendant deux journées pour un prix pouvant aller jusqu'à 2000 euros par personne. L'impact en termes d'organisation et de coût s'avère en effet prohibitif.

2) Autres moyens de gestion des risques

FORTRESS :

S'appuyant sur des animations ludiques (20 animations), il permet de rapidement identifier le niveau de sensibilisation des équipes internes de l'entreprise.
En option, une base de données centralisée permet de suivre les évolutions du degré de sensibilisation et de mettre au point un tableau de bord détaillé.
Cet outil permet au responsable sécurité et/ou au directeur de la formation de déclencher des actions complémentaires d'information à destination des utilisateurs le nécessitant.

HAPSIS : propose une offre originale et ludique de sensibilisation des utilisateurs par un jeu de rôle : SensiRisk.

En effet, la sensibilisation menée sous forme de jeu de rôle favorise l'attention et la mobilisation des participants, entraîne l'implication, stimule l'imagination et la réactivité, et, a un meilleur impact sur une réelle prise de conscience des enjeux. Elle provoque un changement des comportements.

Bénéfices de Sensirisk :
- Pouvoir éducatif du jeu;
- Impact maximal sur l'amélioration du comportement;
- Impact sur l'image de la SSI et de ses représentants;
- Prise en compte des différents aspects de la sensibilisation;
- Possibilité de personnalisation totale.

SensiRisk vous permet de disposer d'un outil de sensibilisation dont vous pouvez faire usage selon votre organisation pour seulement quelques euros par utilisateurs.
En effet, HAPSIS commercialise son offre sous forme de formation ou de licences d'utilisation de SensiRisk. Vous pouvez ainsi disposer de votre outil d'animation de votre formation en interne.
Il est également à noter que SensiRisk est ouvert et permet une adaptation à vos particularités et l'intégration de vos supports (films, slides…).
Mélangeant des questions de culture générale, et comportementale, les participants seront placés dans divers scénarios basés sur l'expérience des consultants de Hapsis et sur le guide des « bonnes pratiques » ISO-17799.

CONCLUSION

ANNEXE