Mini-Rapport d'Audit basé sur la méthode d'analyse MEHARI

Sommaire

I/ Préambule

Nous avons décidé d'appliquer ou du moins, essayé d'appliquer, la méthode MEHARI à notre projet.

Cette méthode est très complète voir trop pour le cadre de notre projet. C'est pourquoi nous nous sommes limités à la définition de l'existant, à un questionnaire adapté et à une rapide analyse en fonction des recommandations de la norme ISO 17999:2005, référence sur la gestion de la sécurité informatique.

L'analyse par une méthode d'audit n'était pas obligatoire dans le projet. Cependant, il nous apparaissait intéressant d'essayer de prendre en main un outil complet d'analyse.

Ci-dessous, les principales méthodes d'audit :

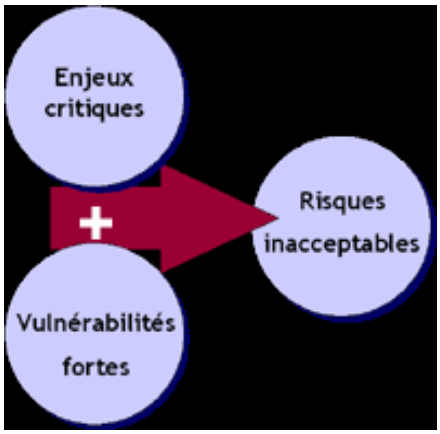
Les principales méthodes d'audit de sécurité			
Nom	**Signification**	**Origine**	**Caractéristiques**
Cobit	Control objectives for information and technology	ISACA	Méthode accessible à tous, dans un langage simple. Les outils fournis permettent la mesure des performances mais la méthode est aujourd'hui davantage assimilée à une méthode de gouvernance des SI.
Ebios	Expression des Besoins et Identification des Objectifs de Sécurité	DCSSI	Notamment déployée au sein de l'administration française, cette méthode comprend une base de connaissances et un recueil de bonnes pratiques. Elle est téléchargeable sur le site de la DCSSI et s'accompagne d'un logiciel.
Feros	Fiche d'Expression Rationnelle des Objectifs de Sécurité	SCSSI	Pas une méthode à proprement parler mais un document permettant à une autorité donnée (secteur secret défense notamment) de définir le niveau d'engagement de sa responsabilité dans l'application d'une politique de sécurité.
Marion	Méthodologie d'Analyse de Risques Informatiques Orientée par Niveaux	CLUSIF	Fonctionne par questionnaires débouchant sur 27 indicateurs répartis en 6 catégories. 2 phases (audit des vulnérabilités et analyse des risques) permettent la définition et la mise en œuvre de plans d'actions personnalisés.
Mehari	Méthode Harmonisée d'Analyse de Risques	CLUSIF	Succède à la méthode Marion. S'articule autour de 3 plans. Permet désormais d'apprécier les risques au regard des objectifs "*business*" de l'entreprise.

Nous avons choisi la méthode MEHARI car d'une part, elle est l'évolution de la méthode MARION et d'autre part, elle est gratuite.

II/ Présentation de la méthode MEHARI

La méthode MEHARI (Méthode Harmonisée d'Analyse des Risques) a été développée par le CLUSIF (Club de la Sécurité des Systèmes d'Information Français) pour cerner les risques liés à l'information.

Cette méthode fournit un cadre, des procédés et des bases de connaissances permettant de se pencher sur plusieurs points tels que:



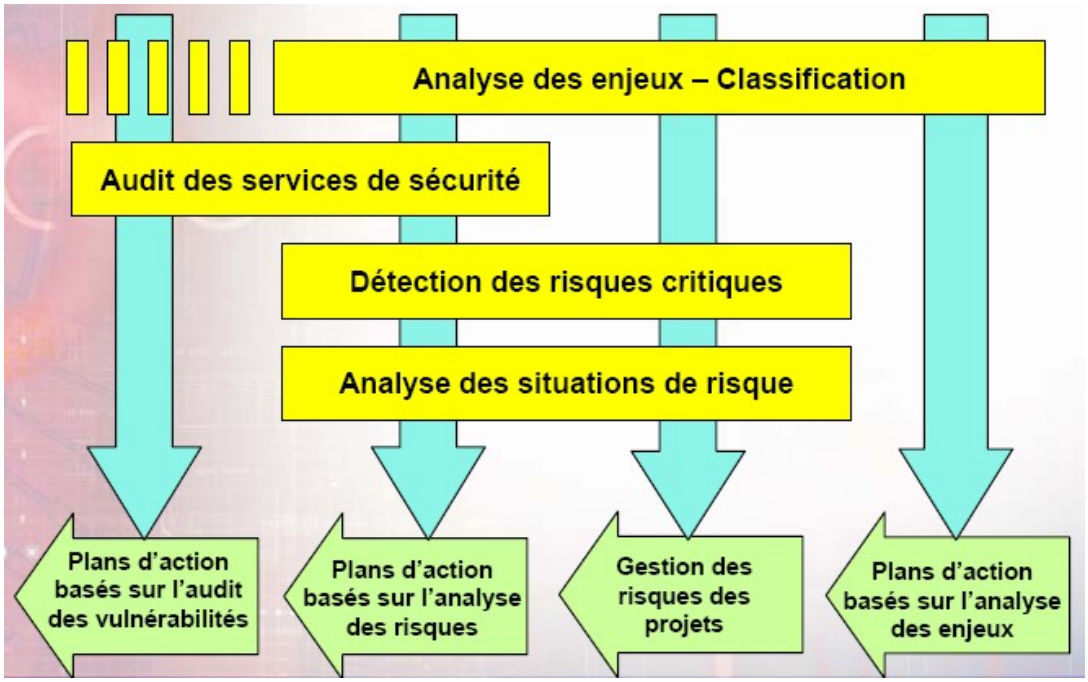
- Les enjeux majeurs de l'entreprise et notamment les dysfonctionnements potentiels et la gravité de ces derniers,

- Les vulnérabilités, en évaluant la qualité des mesures de sécurités en place,

- Les risques de manière à définir les mesures les mieux adaptées à mettre en œuvre.

L'entreprise auditée se soumet à un certain nombre de questionnaires débouchant sur différentes notes de 0 à 4 (en tout, 27 indicateurs répartis en 6 catégories) évaluant sa performance à la fois par rapport à un standard - jugé satisfaisant - mais aussi par rapport aux autres entreprises ayant procédé à l'audit.

Le schéma ci-dessous résume la démarche MEHARI :



III/ Définition et classification des éléments du projet

La première étape a été de définir avec Mr BOSCARI, Chef de projet de la Défense, et Mr ABOUZEID, Responsable de la Communication, les différents domaines d'activités et les processus sensibles (*Annexe 1_Processus majeurs*).

Nous avons ensuite demandé aux responsables quel serait l'impact sur « l'entreprise » en cas de dysfonctionnements d'un des processus. (*Annexe 2_Impact*)

Il a fallu ensuite définir les seuils de gravité pour chaque critère d'impact (*Annexe 3_Seuils d'impacts*) sachant que :

- Seuil 1 : Sans dommage significatif
- Seuil 2 : Dommage important
- Seuil 3 : Grave dommage
- Seuil 4 : Dommage extrêmement grave

Nous avons ensuite recensé et classifier les ressources suivant trois critères :

- Disponibilité
- Intégrité
- Confidentialité

Les notes sont comprises entre 1 et 4 sachant que, plus le critère paraissait important, plus la note était élevée. (*Annexe 4_Classification des ressources*)

IV/ Décomposition du questionnaire

Une fois ces classifications terminées, nous nous sommes appuyés sur les questionnaires de la méthode MEHARI, basé sur 12 scénarii, pour modeler un questionnaire d'environ 400 questions, découpé en six domaines et pour donner un léger aperçu de ce que pourrait être un audit.

Voici les six domaines identifiés :

- **Domaine d'Organisation**
- **Domaine des Locaux**
- **Domaine du Réseau Local (LAN)**
- **Domaine de l'Exploitation des Réseaux**
- **Domaine de la sécurité des Systèmes et de leur architecture**
- **Domaine de la Protection de l'Environnement de Travail**

Pour chaque question, le responsable devait répondre par « oui » ou par « non ».

A la suite de ça, nous nous sommes penchés sur les réponses négatives pour mettre en lumière les non-conformités par rapport à la norme ISO 17999: 2005 et proposés, quand cela était possible, quelques améliorations.

Vous trouverez dans un fichier Excel annexe (*Questionnaire-Résultat et Norme ISO 17999.xls*) les résultats du questionnaire et les différents paragraphes numérotés de la normes ISO.

V/ Recommandations (norme ISO 17999)

Ces recommandations sont tirées des intitulés des paragraphes de la norme ISO 17999 :2005. Les paragraphes concernés sont indiqués entre parenthèse au début de chaque domaine.

a. Domaine d'Organisation

(Par. 06 ; Par. 07 ; Par. 08 ; Par. 10 ; Par. 11 ; Par. 15)

On se place ici dans le cas où le projet aurait comporté des utilisateurs lambda au sein de l'entreprise. Une charte informatique plus complète aurait alors été rédigée.

Le domaine d'organisation mériterait d'être remis en concordance avec les exigences légales et notamment en ce qui concerne la protection des enregistrements. Un paragraphe dans la charte informatique pourrait être crée à cet usage.

Au niveau du contrôle d'accès et de la gestion de l'accès utilisateur, on relève forcément quelques soucis. Il faudrait clairement définir les responsabilités des utilisateurs, le contrôle d'accès au réseau et l'authentification des utilisateurs pour les connexions externes.

En ce qui concerne la gestion de l'exploitation et des télécommunications, les échanges des informations pourrait être plus clairement définis. Pour bien faire, il faudrait établir une politique d'échange avec les procédures inhérentes à cette politique, autour des manipulations des supports amovibles et de la manipulation des informations.

De même, dans un cas réel, on pourrait améliorer la gestion des biens en classifiant les différentes informations.

b. Domaine des Locaux

(Par. 09)

Il s'agit là du plus gros point noir de l'analyse.

En effet, les installations (bâtiments et salles) appartenant à l'université, elles sont, par définition, ouvertes à tous.

On comprend pourquoi la sécurité physique ne permet pas de définir des zones sécurisées avec un périmètre de sécurité adéquat.

De même, la sécurisation et la protection du matériel et du câblage ne peut être correctement réalisé car le choix de l'emplacement n'est pas maitrisé.

c. Domaine du Réseau Local (LAN)

(Par. 10 ; Par. 11)

Au niveau du contrôle d'accès, il est possible d'améliorer la gestion des privilèges en mettant en place un réexamen des droits d'accès utilisateurs sous un contrôle strict.

Il faudrait aussi que la matérialisation des profils, attribués aux utilisateurs sous forme de tables, soit strictement sécurisée. Et que, lors de leur transmission et de leur stockage, il existe un contrôle d'accès renforcé pour pouvoir les modifier, et que ces modifications soient journalisées et auditées.

Au niveau de la gestion de l'exploitation et des télécommunications, il serait intéressant de mettre en place une surveillance plus accrue avec par exemple des rapports de défaut régulier.

De même, en ce qui concerne la sauvegarde des informations, il faudrait réaliser un plan de sauvegarde et un plan de reprise d'activité du réseau local.

d. Domaine de l'Exploitation des Réseaux

(Par. 15)

Au niveau de la conformité, il faudra auditer le système d'information et la protection des outils système d'information au moins une fois par an et ce, avec un contrôle strict s'appuyant sur un logiciel validé et subissant régulièrement un test d'intégrité.

e. Domaine de la sécurité des Systèmes et de leur architecture

(Par. 10)

Pour la gestion de l'exploitation et des télécommunications, la surveillance par filtrage d'accès et par règles pourraient spécifier, pour chaque type d'accès (système, SGBD, etc.), les éléments fondamentaux à enregistrer, par exemple l'identifiant, la date et l'heure, etc.

La manipulation des supports, et notamment la mise au rebut de ces derniers, pourrait être spécifiée dans un document stipulant clairement l'obligation de non divulgation des données jusqu'à leur destruction.

f. Domaine de la Protection de l'Environnement de Travail

(Par. 06 ; Par. 10 ; Par. 11)

S'il existait une charte pour les utilisateurs, le contrôle d'accès devrait être bien spécifié et les utilisateurs averti de ne pas laisser leur poste sans surveillance. Il faudrait aussi tenir compte de la gestion des échanges d'informations notamment par messagerie électronique. Et se pencher sur les autorisations concernant le travail distant.

VI/ Conclusion

L'analyse pourrait être plus approfondie avec le calcul de différents indicateurs tel que la métrique de risque, de dissuasion, de potentialité, etc.

Néanmoins, cela nous paraissait inutile car la base de questionnaire ayant été modifiée, les calculs qui en découlent se trouvent biaisés. De plus, compte tenu du nombre important de projets que nous avions à réaliser, nous n'aurions pas eu le temps de rentrer plus amplement dans les détails.

Quoiqu'il en soit, on a donc pu voir, par ce mini-audit, que le point le plus critique du projet était le domaine des locaux.

Il est d'autant plus critique qu'il a joué un rôle important lors du projet. En effet, avec un contrôle physique des accès et une sécurisation des salles plus accrue, les Attaquants, lors de la confrontation du 04 décembre 2007, n'auraient pas pu installer de keyloggers sur des postes de la salle 213.

Pour conclure, il était intéressant d'essayer de prendre en main une méthode d'audit malgré la difficulté inhérente. Les cabinets d'audits étant de plus en plus convoités par les entreprises pour obtenir une évaluation de leur système informatique, on sera peut être amené, dans un futur proche, à travailler au sein d'un de ces cabinets ou à faire appel à l'un d'eux.

Il devient donc avantageux de connaitre les méthodes et démarches utilisées.

VII/ Annexes

Annexe 1_Processus majeurs

Processus majeurs de l'entreprise			
Domaines	**Processus**	**Description**	**Sensibilité**
Management	Prise de décision	Respect des délais Assignement des taches	**
	Gestion du projet	Suivi du projet et diagramme de Gantt	*
Juridique & commercial	Gestion du contrat et du Cahier des charges	Communication interne/externe Elaboration du contrat Respect du contrat et des accords	**
Sécurité	Politique de sécurité	Elaboration de la politique Gestion et suivi de la politique	**
Direction Technique	Techniciens	Installation réseau Gestion du réseau Exploitation des serveurs Gestions des postes clients	****
	Responsable	Interface techniciens/décisionnaire Elaboration du plan d'adressage	***

Annexe 2_Impact

Impacts	
Domaines	**Description de l'impact**
Management	Retard dans le projet Perte de synchronisation entre les membres de l'équipe
Juridique & commercial	Perte de temps si mauvaise transmission des informations Mise en danger des installations si le retard apparaît trop important
Sécurité	Possibilité d'intrusion au réseau devient plus importante Vol d'information Mauvais fonctionnement du réseau
Direction Technique	Arrêt des équipements et des services Intrusion facilité si mauvaise configuration Vols d'information

Annexe 3_Seuils d'impacts

Seuils d'impacts					
Domaines	**Types d'impacts**	**Seuils**			
		Gravité 1	**Gravité 2**	**Gravité 3**	**Gravité 4**
Management	Retard du projet	< 3jours	entre 5 jours et 10 jours	entre 10 jours et 20 jours	> 20 jours
	Perte de synchronisation de l'équipe	Absence temporaire	> 1 semaine	> 2 semaines	> 1 mois
Juridique & commercial	Mauvaise transmission des infos	informations non importantes	Causant une interruption de services temporelle	informations relatives à l'organisation de l'équipe et du réseau	informations importantes comme une intrusion non relégué
	Oublis dans le contrat	exception	avenant important	avenant très important	contrat non conforme
Sécurité	Faille dans la politique de sécurité	laxisme sur le suivi		indisponibilité du réseau	Divulgation d'informations
Direction Technique	Arrêt des services	1/2 journée	1 à 2 jours	3 à 4 jours	> 5 jours
	Arrêt du réseau	1 heure	1/2 journée	1 jour	> 2 jours
	Intrusion			compromission des machines	vol d'information

Annexe 4_Classification des ressources

Classification des ressources				
Nom	**Type**	**Disponibilité**	**Intégrité**	**Confidentialité**
Site de Paul Sabatier	Bâtiment	1	1	1
Local réseau	U2-213	2	2	2
Réseau	Ethernet	3	3	4
Serveur	Système	2	3	4
Personnel	RH	3	4	2