14 mars 2013

Les Plans de Sécurité Informatique

Dossier Final

Adrien THIERY
Jean-Baptiste CLAVEL

Table des matières

I. Introduction au sujet de la sécurité informatique :

Définition :
La sécurité des systèmes d'information (SSI) est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaire et mis en place pour conserver, rétablir, et garantir la sécurité du système d'information. Assurer la sécurité du système d'information est une activité du management du système d'information.

1. Quels enjeux et quels risques ?

Plusieurs types d'enjeux doivent être maitrisés :

- **L'intégrité** : Les données doivent être celles que l'on s'attend à ce qu'elles soient, et ne doivent pas être altérées de façon fortuite ou volontaire.
- **La confidentialité** : Seules les personnes autorisées ont accès aux informations qui leur sont destinées. Tout accès indésirable doit être empêché.
- **La disponibilité** : Le système doit fonctionner sans faille durant les plages d'utilisation prévues, garantir l'accès aux services et ressources installées avec le temps de réponse attendu.
- **La non-répudiation et l'imputation** : Aucun utilisateur ne doit pouvoir contester les opérations qu'il a réalisées dans le cadre de ses actions autorisées, et aucun tiers ne doit pouvoir s'attribuer les actions d'un autre utilisateur.
- **L'authentification** : L'identification des utilisateurs est fondamentale pour gérer les accès aux espaces de travail pertinents et maintenir la confiance dans les relations d'échange.

La sécurité informatique est un défi d'ensemble qui concerne une chaine d'éléments : Les infrastructures matérielles de traitement ou de communication, les logiciels (systèmes d'exploitation ou applicatifs) , les données , le comportement des utilisateurs . Le niveau global de sécurité étant défini par le niveau de sécurité du maillon le plus faible, les précautions et contre-mesures doivent être envisagées en fonction des vulnérabilités propres au contexte auquel le système d'information est censé apporter service et appui.

On distingue trois types de sécurité :

Sécurité humaine

Un centre regroupant un ou plusieurs serveurs hébergeant les informations sensibles d'une entreprise est une cible de choix pour des êtres mal intentionnés. C'est pourquoi la sécurité des accès doit être surveillée au mieux. Pour une sécurité des informations maximale, la présence humaine continue (gardiennage 24/24) peut être renforcée par un système de vidéo surveillance, de régulation d'entrées/sorties par badges et d'alerte anti-intrusion déployé dans l'ensemble de ce bâtiment.

Sécurité physique et matérielle

Pour éviter la destruction des informations en cas de destruction d'un serveur, les équipements déclarés comme sensibles doivent être systématiquement redondés, c'est-à-dire dupliqués en un ou plusieurs endroits. Il existe aujourd'hui des systèmes et des techniques de sauvegarde de données régulières afin d'éviter les pertes de données imprévues (par exemple le fonctionnement de deux disques miroirs via RAID1 (Redundant Array of Independent Disks) ou l'utilisation de scripts de sauvegarde automatique).
Pour résister à une coupure (criminelle ou non) de ressources, un centre de serveurs se doit aussi de bénéficier d'une autonomie électrique régulièrement testée en cas de coupure électrique. Il peut aussi bénéficier d'un système de sécurité incendie ainsi que d'un groupe de refroidissement autonome adapté pour réguler au mieux la température des serveurs et en protéger le matériel, même en cas de coupure d'eau.

Sécurité logicielle

Pour bien protéger son système d'information, il est nécessaire de protéger son système de toutes les attaques logicielles.

Il existe trois catégories d'attaques :

- les attaques qui permettent d'obtenir des informations ou des privilèges pour mener un autre type d'attaque. On parle d'attaque par rebond.
- les attaques simultanées par collusion : technique qui consiste à déclencher de nombreuses attaques de manière coordonnée. Cette technique est notamment utilisée pour l'analyse de cryptogramme.
- les attaques simultanées par coordination sur une cible unique : il s'agit de coordonner une attaque utilisant de très nombreux systèmes pour saturer la cible.

Voici les principales attaques logicielles connues à ce jour. Cette liste n'est bien sûr pas exhaustive :

- Brouillage : attaque de haut niveau utilisant les rayonnements électromagnétiques qui rendent le SI inopérant.
- Écoute : sauvegarde des informations qui transitent sur un réseau informatique ou de télécommunication.
- Cryptanalyse : attaque d'un chiffre. Pour assurer cette attaque, d'excellentes connaissances en mathématiques et une forte puissance de calcul sont requises.
- Mystification : simulation de la part de l'attaquant du comportement d'une machine pour tromper un utilisateur. Par exemple, *un terminal de paiement invitant à entrer ses données bancaires confidentielles*
- Trappe (ou Backdoor) : point d'entrée dans une application placée par un développeur.
- Asynchronisme : exploitation du fonctionnement asynchrone de certaines parties ou commandes du système d'exploitation.

- Souterrain : type d'attaque qui évite de s'attaquer directement à une protection mais qui tente de s'en prendre à un élément qui la supporte.
- Salami : acquisition imperceptible de données parcellaires d'un SI en vue de les rassembler et d'obtenir un tout exploitable.
- Balayage (scanning) : cette technique consiste à envoyer au SI un ensemble de requêtes de natures diverses afin d'examiner les réponses du système. En automatisant ces sollicitations du SI, le pirate pourra facilement trouver le nom de certains utilisateurs et pourquoi pas leur mot de passe.
- Exploitation d'un défaut (bug) : De nombreuses failles sont présentes dans les logiciels commerciaux. Ces failles sont exploitées à des fins malveillantes par les pirates.
- Logiciel espion (spyware) : logiciel malveillant infectant un ordinateur dans le but de collecter et de transmettre, de manière invisible, des informations de l'environnement sur lequel il est installé.
- Canal caché : Attaque de très haut niveau permettant de récupérer des informations en violant la politique de sécurité. Il existe 4 canaux cachés :
    - les canaux de stockage pour le transfert/la récupération d'informations
    - les canaux temporels pour étudier les temps de réponse du SI
    - les canaux de raisonnement qui permettent à un processus de déduire de l'information à laquelle il n'a pas normalement accès
    - les canaux dits de "fabrication" qui créent de l'information fausse.
- Réseau de robots logiciels (botnet) : Réseau de robots logiciels (bots) installés sur énormément de machines. Ces robots se connectent sur des serveurs IRC (Internet Relay Chat) à partir desquels ils reçoivent des instructions de type : envoi de spam, vol d'informations, participation à des attaques de saturation…
- Perturbation : L'agresseur va essayer de fausser le comportement du SI ou de l'empêcher de fonctionner en le saturant, en modifiant ses temps de réponse ou en provoquant des erreurs. L'agresseur veut désorganiser, affaiblir ou ralentir le système cible.
- Saturation : technique consistant à remplir une zone de stockage ou un canal de communication jusqu'à ce que l'on ne puisse plus l'utiliser.
- Pourriel (spam) : courrier électronique indésirable transmis à une multitude de destinataires envoyés sans que l'émetteur ne soit au courant. Le spam contribue à la pollution voir à la saturation des boîtes aux lettres électroniques.
- Canular (hoax) : rumeur propagée, souvent par courrier électronique, comme quoi un virus catastrophique circule sur la toile, virus imaginaire bien évidement. Ce n'est pas une réelle attaque mais cela contribue à la désinformation générale.
- Hameçonnage ou filoutage (phishing) : Technique simple qui permet d'obtenir des informations confidentielles telles que les mots de passe en se faisant passer auprès des victimes pour quelqu'un digne de confiance. Par exemple, une banque qui demande des codes confidentiels...
- Les virus : Un virus informatique est un logiciel malveillant conçu pour se propager à d'autres ordinateurs en s'insérant dans des programmes légitimes appelés « hôtes ». Il peut perturber plus ou moins gravement le fonctionnement de l'ordinateur infecté.

- Les vers : Un ver, contrairement à un virus informatique, n'a pas besoin d'un programme hôte pour se reproduire. Il exploite les différentes ressources de l'ordinateur qui l'héberge pour assurer sa reproduction et a habituellement un objectif malfaisant.
- Les chevaux de Troie : logiciel d'apparence légitime, conçu pour exécuter des actions à l'insu de l'utilisateur.

Cet arsenal d'attaques représente une partie des menaces potentielles pour un système. Un système doit donc nécessairement se prémunir contre ces différentes attaques.

2. Quelles conséquences ?

Une organisation dont le système d'information est piraté est affectée de deux façons :

- par des **dommages financiers** directs (comme le fait d'avoir à reconstituer des bases de données qui ont disparu, reconfigurer un parc de postes informatiques, réécrire une application) ou indirects (par exemple, le dédommagement des victimes d'un piratage, le vol d'un secret de fabrication ou la perte de marchés commerciaux). Par exemple, bien qu'il soit relativement difficile de les estimer, des sommes de l'ordre de plusieurs milliards de dollars US ont été avancées suite à des dommages causés par des programmes malveillants comme le ver Code Red.
- par la perte ou la baisse de **l'image de marque**. Perte directe par la publicité négative faite autour d'une sécurité insuffisante (cas du hameçonnage par exemple) ou perte indirecte par la baisse de confiance du public dans une société. Par exemple, les techniques répandues de defacing (une refonte d'un site web) permettent à une personne mal intentionnée de mettre en évidence des failles de sécurité sur un serveur web. Ces personnes peuvent aussi profiter de ces vulnérabilités pour diffuser de fausses informations sur son propriétaire (on parle alors de désinformation).

Penchons-nous désormais sur deux exemples afin d'illustrer notre propos : le cas du piratage du PlayStation Network (alias PSN) de Sony et celui des Heartland Payment systems.

Le hack du PSN

L'origine de cette attaque est assez lointaine puisqu'elle trouve sa source dans l'homme qu'est George Francis Hotz (ou GeoHot, pour les intimes… et tout internet). GeoHot est connu dans le monde du hacking notamment pour avoir jailbreaké (piraté) l'iPhone, mais surtout, dans le cas qui nous concerne, pour être le premier à avoir cracké la Playstation 3, en 2010. GeoHot a notre âge, 23 ans, et est un petit génie de l'informatique et de l'électronique, hacker de profession. C'est pourquoi, quand il a acheté sa nouvelle console Playstation, GeoHot a trouvé amusant d'essayer d'en obtenir le maximum, et notamment dans le cas présent, il a voulu avoir accès au système d'exploitation très fermé et sécurisé de la console.
Cependant, en rendant public les informations sensibles, et notamment la "Master Key" de la PS3 (clé de cryptage), GeoHot s'est attiré les foudres de l'entreprise japonaise qui a alors porté plainte contre lui sous une multitude de chefs d'accusation. Pour appuyer son attaque en

justice, la société se débrouille pour qu'une descente soit réalisée dans le logement de GeoHot et que tout son matériel informatique soit détruit. Et là, c'est le drame.
Cette attaque fait le buzz (ou le ramdam, si on s'en tient aux consignes de l'académie française) et attire l'attention des Anonymous, un groupe de hacktiviste bien connu sur internet. Se reconnaissant dans la personne de GeoHot, ces derniers ripostent à l'action de Sony en attaquant son réseau de jeu en ligne, le fameux PSN et le service Qriocity(service de Streaming de musique et de Vidéos à la demande de Sony), rendant inaccessible un certain nombre de sites de l'entreprise et dérobant des informations confidentielles sur pas moins de 25 millions de clients de Sony (les informations n'étant pas chiffrées). On parle ici de données personnelles des clients de Sony : noms, adresses et adresses électroniques, dates d'anniversaire, pseudonymes et mots de passe, historiques des paiements, factures ainsi que des données plus sensibles telles que les données bancaires.
Sony coupe alors l'ensemble du PSN et de Qriocity le 20 avril 2011 pour une maintenance qui durera jusqu'au 16 mai 2011.
Les conséquences sont lourdes pour Sony : des millions de dollars perdus (on parle de 170 millions de dollars de pertes), des millions d'utilisateurs mécontents, des actions en justice engagées contre l'entreprise pour négligence de failles de sécurité, l'action de Sony chute et… les ingénieurs sécurité de chez Sony qui passent pour des imbéciles. En effet, il semblerait que Sony utilisait des versions obsolètes de logiciels et que ses serveurs n'étaient pas protégés par un pare-feu.
De l'importance de bien protéger et de crypter les données à caractère personnel et de mettre à jour le logiciel (Apache) de vos serveurs…

Heartland Payment Systems

En 2009, Heartland Payment Systems est l'un des plus grands organismes de transferts de paiements aux Etats Unis. Malgré son importance, la société est victime d'une faille informatique découverte et exploitée largement par le pirate Albert Gonzalez et deux associés via un spyware implanté sur l'un des serveurs de la société, puisqu'ils ont pu ainsi accéder aux données (nom, numéros de cartes, dates d'expiration et monitoring des crédits et débits) de plus de 130 millions de cartes de crédit. Les hackers ne pouvaient cependant pas utiliser les informations telles quelles mais pouvaient créer de fausses cartes de crédit avec les données volées.
Le 25 mars 2010, un tribunal américain a condamné le pirate à purger une peine de prison de 20 ans et un jour, ainsi qu'à 25.000 dollars d'amende, voulant faire un exemple pour décourager ce genre de crimes. A titre de comparaison, les pertes de Heartland Payment Systems s'élèveraient à 12,8 millions de dollars.
De l'utilité de surveiller ses machines et les protéger avec les programmes adéquats.
Dans le prochain article, nous ferons donc une synthèse de notre travail et un résumé des bonnes pratiques à avoir afin d'obtenir une sécurité informatique minimale.

II. Les plans de sécurité informatique

Problématique :

Comment améliorer et formaliser la sécurisation de nos systèmes informatiques ?

I. Origine & concept

Depuis le début des années 2000, la sécurité informatique est devenue de plus en plus importante et c'est cette nécessité d'un système toujours plus sûr qui nous a incité à essayer de répondre à notre problématique ci-dessus. C'est aussi cela qui a donné naissance à la notion centrale de notre étude : **les plans de sécurité informatique**.

En effet, les réseaux d'entreprise sont aujourd'hui nécessaire à son fonctionnement. Leur sécurité est donc primordiale et afin de protéger au mieux ces systèmes multi-plateformes et de plus en plus décentralisés, il est nécessaire de trouver et de mettre en place une stratégie permettant d'**inspecter**, **protéger**, **détecter**, **réagir** et **réfléchir** le plus efficacement possible sur le thème de la sécurité des systèmes informatiques qui interagissent dans le réseau de l'entreprise.

II. La norme ISO 17799

La norme ISO 17799 constitue les « best practice », les règles de bonnes conduites à suivre et les objectifs à atteindre pour avoir une bonne sécurité informatique et permet donc de cadrer officiellement les plans de sécurité informatique.

<u>Présentation de la norme ISO 17799</u>

Internationale, la norme ISO 17799, crée en 2005, établit des lignes directrices et des principes généraux pour préparer, mettre en œuvre, entretenir et améliorer la gestion de la sécurité de l'information au sein d'un organisme.
Ce code de bonne pratique est subdivisé en différentes 10 chapitres (cf ci-dessous).

Représentation des 10 chapitres de la norme ISO 17799 sous forme de pyramide

Chapitre 1 : Politique de sécurité

La politique de sécurité donne des définitions claires de la sécurité de l'information (SI), une explication des principes de sécurité, évoque l'implication de la direction de l'organisme et les modalités de déclaration des incidents de sécurité.
On retiendra que les facteurs clé de succès de la mise en œuvre d'une politique de sécurité de l'information sont :

- la mise en œuvre de la gestion de la SI compatible avec la culture de l'organisation
- un soutien et un engagement réel et visible de la direction de l'organisme
- une bonne compréhension des exigences de sécurité
- une bonne communication interne (auprès des employés et des responsables) (présentation – formations – campagnes de sensibilisation)
- une bonne communication externe de la politique de SI (auprès des fournisseurs par exemple)
- un système de mesures pour évaluer l'efficacité de la gestion de la sécurité

Chapitre 2 : Organisation de la sécurité

Des groupes de travail devront être mis en œuvre, avec l'appui de la direction, pour approuver la politique de sécurité de l'information, pour assigner des rôles de sécurité et pour coordonner la sécurité dans l'organisme.

Chapitre 3 : Classification et contrôle des actifs

La norme préconise qu'un propriétaire soit identifié pour chaque actif principal (exemple: Données client, données achat, …) de façon à s'assurer qu'un niveau de protection approprié de cet actif soit mis en œuvre. Ce propriétaire d'information sera responsable de la mise en œuvre des contrôles appropriés et même si la réalisation des contrôles peut être déléguée, la responsabilité finale vis-à-vis de cet actif devra demeurer chez le propriétaire désigné.
Le processus de réalisation de l'inventaire des actifs est un aspect important de la gestion des risques. Un organisme doit pouvoir identifier ses actifs, ainsi que leur valeur et importance relatives.

Chapitre 4 : Sécurité liée au personnel

La norme ne se réduit pas à une norme technique, elle met beaucoup l'accent sur la culture de la sécurité de l'entreprise et notamment celle liée à son personnel, notamment lors de la procédure de recrutement, des contrats d'embauche et de la formation à la sécurité (connexions et déconnexion aux applicatifs, politique de mots de passe, signalement des incidents de sécurité, processus disciplinaire).

Chapitre 5 : Sécurité physique et de l'environnement

Sécurité Physique :
La sécurité physique est un sujet de fond dans la sécurité de l'information. La norme préconise la création de différents niveaux de sécurisation de zone, la mise en place de systèmes de contrôle d'accès, la séparation des zones de livraison…

Sécurité du matériel informatique :
La norme aborde les thèmes liés à la sécurité des serveurs et de leur environnement (gestion des alimentations électriques, politique pour limiter l'utilisation de boisson et de nourriture, procédure de sortie des matériels informatiques des locaux…)
Des points plus sensibles sont abordés comme par exemple : comment effacer définitivement les données ?

Chapitre 6 : Sécurité de l'exploitation et des réseaux

Dans ce chapitre, deux grands thèmes sont décrits :

- les thèmes liés à la sécurisation de l'exploitation de l'information (évolutions des systèmes d'information, gérer les incidents de sécurité, séparation des fonctions à risques…)
- la sécurité des réseaux au sens large véhiculant l'information, notamment toute la sécurité des échanges et les moyens associés (scellement, cryptographie, signature électronique…)

Chapitre 7 : Contrôles d'accès logique

Ce chapitre décrit la politique à mettre en œuvre pour structurer la gestion des accès au système d'information pour les utilisateurs de l'organisme, mais également pour les systèmes externes qui se connectent automatiquement à des applications.
Deux thèmes sont abordés :

- la gestion des mots de passe
- la gestion des accès logiques

Chapitre 8 : Développement et maintenance des systèmes d'information

Ce chapitre traite des infrastructures informatiques, des applications de l'entreprise et également des applications développées par les utilisateurs. Mais aussi de la politique sur l'utilisation des mesures cryptographiques : cette partie décrit l'ensemble du processus organisationnel à mettre en œuvre pour assurer une bonne utilisation du cryptage, des signatures numériques, des services de non répudiation et de la gestion des clés.

Chapitre 9 : Continuité d'activité

Quelles que soient les probabilités de risques, les dirigeants doivent pouvoir engager des moyens pour garantir la continuité de l'activité et en particulier, la permanence de la relation client. Sans système d'information, l'entreprise a en effet bien du mal à réorganiser ses processus. Cette conception dépasse la reprise sur le seul sinistre du système d'information : elle vise à réunir pour chaque collaborateur un emplacement de travail, un téléphone, et un poste de travail.

Chapitre 10 : La gestion de la conformité

Comme l'ISO 177999 est une norme internationale, l'identification de la législation applicable au pays est la première tâche. Il convient ensuite de définir explicitement et documenter les exigences légales, réglementaires et contractuelles pour chaque système d'information. (propriété intellectuelle, droits d'auteur, copyright des logiciels, protection des données personnelles…)

Les plans de sécurité informatique sont nécessaires aux entreprises afin de protéger leurs systèmes et sont prônés et encouragé par les états. Mais comment une entreprise voulant sécuriser son système d'information ? C'est ce que nous allons découvrir tout de suite.

III. Quels outils pour les plans de sécurité informatique ?

1. Les méthodes d'audit

Il existe un certain nombre de méthodes permettant d'auditer et de sécuriser un système d'information. Le lecteur avide de savoir anglophone pourra notamment s'intéresser à la norme OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), mais nous avons trouvé que l'étude de cette méthode n'était pas nécessaire pour cet article et avons préféré nous intéresser aux méthodes suivantes :

La "méthode" Feros (Fiche d'Expression Rationnelle des Objectifs de Sécurité)

Lors de nos recherches, nous avons vu la "méthode FEROS" évoquée quasiment au même niveau que les méthodes EBIOS, MEHARI (ou MARION et MELISA, les méthodes "mères" de MEHARI), alors qu'une FEROS est en fait un document obligatoire (dans le cas de systèmes traitant des informations classifiées de défense) ou recommandé qui consiste à formaliser tous les éléments nécessaires à l'acceptation du système par une autorité. Il présente donc non seulement tous les objectifs de sécurité du système étudié et les risques résiduels, mais aussi la démarche et l'argumentation qui a permis de les identifier.
De plus, la réalisation d'une FEROS est adaptée à l'utilisation de EBIOS, c'est donc ce qu'on pourrait considérer comme une annexe à la méthode EBIOS, même s'il est possible de réaliser une FEROS après avoir utilisé une autre méthode. En décidant de réaliser une FEROS, il faut cependant avoir utilisé une méthode d'audit de sécurité.
Pour conclure, si on sécurise un système d'information grâce à une méthode telle que MEHARI ou EBIOS, l'utilisation de la norme ISO 17799 pourrait faire l'objet d'une utilisation pour la vérification des bonnes pratiques des règles de sécurité établies grâce aux méthodes.

La méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité)

La méthode EBIOS a été développée par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI). Les réflexions de cette méthode sont menées à un niveau davantage fonctionnel que technique et elle fournit les éléments nécessaires à la validation formelle par une autorité de la gestion, la surveillance et la revue des risques.
La méthode se présente en cinq étapes :

1 - L'étude du contexte
2 - L'étude des évènements redoutés
3 - L'étude des scénarios de menaces
4 - L'étude des risques
5 - L'étude des mesures de sécurité

1 – Étude du contexte

Objectif : définir précisément le contexte de l'étude et ses enjeux.
Cette étape permet de formaliser le cadre de gestion des risques, d'identifier, de délimiter et de décrire le périmètre de l'étude, ses enjeux, son contexte d'utilisation, ses contraintes spécifiques…
Cette étape se décompose en trois sous-activités :
– Définir le cadre de la gestion des risques
– Préparer les métriques
– Identifier les biens

2 – Étude des évènements redoutés

Objectif : identifier de manière systématique les scénarios génériques que l'on souhaite éviter concernant le périmètre de l'étude.
Il permet tout d'abord de faire émerger tous les évènements redoutés en identifiant et combinant chacune de leurs composantes : on estime ainsi la valeur de ce que l'on souhaite protéger (les besoins de sécurité des biens essentiels), on met en évidence les sources de menaces auxquelles on est confronté et les conséquences (impacts) des sinistres. Il permet également de recenser les éventuelles mesures de sécurité existantes et ré-estimer la gravité des évènements redoutés, une fois les mesures de sécurité appliquées.

3 – Étude des scénarios de menaces

Objectif : identifier de manière systématique les modes opératoires génériques qui peuvent porter atteinte à la sécurité des informations du périmètre de l'étude (scénarios de menaces).
Il permet tout d'abord de faire émerger tous les scénarios de menaces : on met en évidence les différentes menaces qui pèsent sur le périmètre de l'étude, les failles exploitables pour qu'elles se réalisent (les vulnérabilités des biens supports). Il permet également de recenser les éventuelles mesures de sécurité existantes et ré-estimer la vraisemblance des scénarios de menaces, une fois les mesures de sécurité appliquées.

4 – Étude des risques

Objectif : mettre en évidence de manière systématique les risques pesant sur le périmètre de l'étude, puis de choisir la manière de les traiter en tenant compte des spécificités du contexte.
Il s'agit ici d'identifier les scénarios réellement pertinents vis-à-vis du périmètre de l'étude. Il permet en outre de les qualifier explicitement en vue de les hiérarchiser et de choisir les options de traitement adéquates.
Cette étape est constitué de deux sous-activités :
– Apprécier les risques
– Identifier les objectifs de sécurité

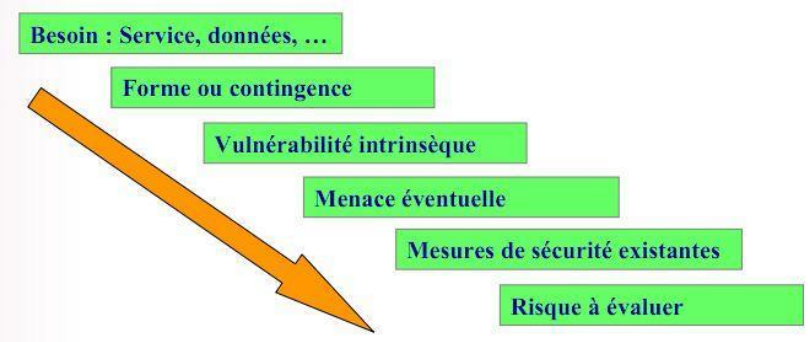
5 – Étude des mesures de sécurité

Objectif : déterminer les moyens de traiter les risques et de suivre leur mise en œuvre.
Il permet de trouver un consensus sur les mesures de sécurité destinées à traiter les risques, d'en démontrer la bonne couverture, et enfin, d'effectuer la planification, la mise en œuvre et la validation du traitement.
Cette étape est constitué de deux sous-activités :
– Formaliser les mesures de sécurité à mettre en œuvre
– Mettre en œuvre les mesures de sécurité
De plus, cette méthode propose un certain nombre d'outils : Des guides pratiques pour mettre en oeuvre la méthode, un logiciel libre et gratuit, une formation, des études de cas et le club EBIOS, une association à but non lucratif qui permet de favoriser les échanges d'expériences, l'homogénéisation des pratiques et la vérification de la satisfaction des besoins des usagers.

La methode MEHARI

MEHARI (MEthode Harmonisée d'Analyse de RIsques) est développée depuis 1995 par le CLUSIF, elle dérive des méthodes Melisa et Marion. Elle est utilisée par de nombreuses entreprises publiques et privées dans sa version française et anglaise.

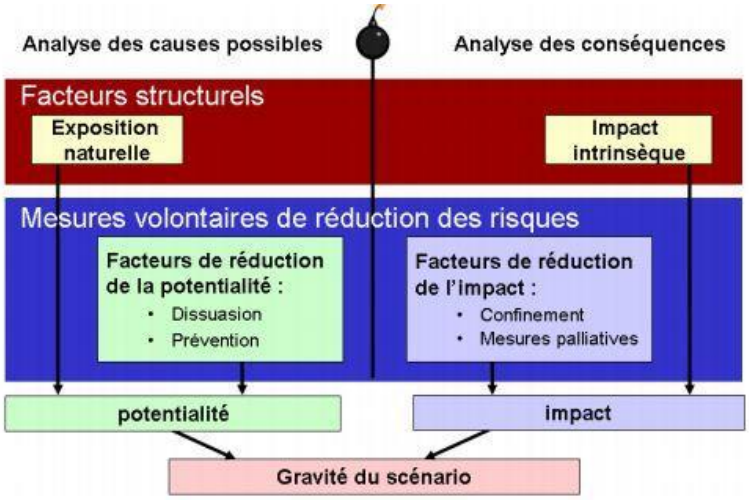
Mehari est basée sur des spécifications s'articulant sur trois grands axes complémentaires :
- *L'identification des risques :* Qui comprend l'identification des actifs, des menaces, des mesures existantes, des vulnérabilités et des conséquences. Cela se fait suivant un processus défini comme suit :



Processus d'identification des risques

Le « besoin de l'activité », point de départ du processus repose sur l'identification des besoins de services, de données (nécessaires aux services) ainsi qu'au besoin de conformité des comportements au référentiel. Après l'identification des actifs dits « primaires », on identifie leurs différentes formes et contingence qui donnent les actifs « secondaires » pour lesquels s'applique le reste du processus jusqu'à préciser les risques à évaluer.

- *L'estimation des risques :* Elle tient compte des facteurs structurels (liés à l'activité de l'organisme), des mesures de sécurité mises en œuvre et de la qualité de ces mesures.
Elle combine l'analyse des causes et des conséquences possibles pour évaluer la gravité d'un scénario suivant sa potentialité et son impact.



Représentation de la démarche d'estimation des risques

- *La gestion des risques :* Elle s'appuie sur les différentes étapes précédentes et vise à répondre aux objectifs déterminés (Services de sécurité à améliorer, niveaux de qualité cibles, etc.…)
Mehari est basée sur trois types de livrables :
- Le Plan Stratégique de Sécurité (PSS) fixe les objectifs ainsi que les métriques qui permettent de les mesurer. Il définit la politique et les grands axes de sécurité du SI pour ses utilisateurs.
- Les Plans Opérationnels de Sécurité (POS) décrivent les mesures de sécurité spécifiques à mettre en œuvre, en élaborant des scénarios de compromission et via un audit des services du SI. Ceci permet d'évaluer chaque risque (probabilité – impact) et par la suite d'exprimer les besoins de sécurité et les mesures de protections.
- Le Plan Opérationnel d'Entreprise (POE) assure le management de risque par la conception d'indicateurs sur les risques identifiés et des scénarios contre lesquels il faut se protéger.

Mehari repose sur un modèle de risque donnant lieu à des métriques pour estimer les paramètres liés aux risques :
- Niveaux de qualité des services.
- Facteurs de réduction de risques.
- Effets de la combinaison des services.
- Estimation de la gravité du risque.
Cependant, il est à souligner que le CLUSIF spécifie le concept de "confiance raisonnée" pour Méhari : les mécanismes de calcul peuvent donner une fausse impression de précision, le modèle reposant sur un principe de prudence…

Comparaison de la méthode EBIOS et de MEHARI.

EBIOS	**MEHARI**
Publié en 1997, créée en 1995	développée depuis 1995
Structure	
Étude du context	*1. L'identification des risques*
Étude des événements redoutés	
Étude des scénarios de menaces	
Étude des risqué	*2. L'estimation des risques*
Étude des mesures de sécurité	*3. La gestion des risques*
Outils	
Guide pratique	*Documents pratiques*
Logiciel libre et gratuity	*Logiciel gratuity*
Formation	*Vidéos*
Etudes de cas	*Outils de calculs Excel intégrés au logiciel*
Club EBIOS	

Finalement, on se rend compte que ces deux méthodes abordent les même sujets, mais peut être sous un angle un peu plus fonctionnel pour la méthode EBIOS et plus "managériale" pour la méthode MEHARI.

2. Les outils des méthodes d'audits

Le logiciel EBIOS

Le logiciel EBIOS constitue un outil très utile dans la mise en place de la méthode du même nom.

Présentation du logiciel EBIOS et de ses fonctionnalités.

Page d'accueil du logiciel EBIOS

Le logiciel EBIOS est donc un logiciel d'assistance à l'utilisation de la méthode EBIOS. Il respecte la philosophie générale de la méthode.
Il permet de créer des livrables conformes aux plans recommandés par la direction centrale de la sécurité des systèmes d'information (DCSSI), notamment les Fiches d'Expression Rationnelle des Objectifs de Sécurité (FEROS), les profils de protection, les cahiers des charges SSI, les politiques de sécurité.
Il permet d'accéder aux bases de connaissances et de les adapter à des contextes particuliers. Les acteurs de la SSI (Direction, RSSI…) peuvent ainsi diffuser des éléments de politique de sécurité tels que les valeurs de l'organisme, la réglementation applicable, l'échelle de sensibilité à utiliser, les menaces à prendre en compte ou les objectifs de sécurité à couvrir.
C'est un outil puissant pour le conseil lié à la gestion des risques SSI. Il permet notamment de :

- consigner les résultats d'une analyse des risques SSI
- gérer un contenu dynamique et interactif
- capitaliser les savoirs pour créer un référentiel propre à l'organisme
- communiquer efficacement les résultats.

De plus, ce logiciel suit les évolutions de la méthode EBIOS, notamment la convergence vers les normes internationales telles que l'ISO 15408.

Voici les différentes fonctionnalités du logiciel :

- **Réalisation d'une étude EBIOS :** permet de consigner les résultats des études, de produire les divers tableaux et d'effectuer certains calculs automatiquement.

1er écran de la réalisation d'une étude EBIOS

La réalisation d'une étude est composée de 6 parties :

- L'étude du contexte : étape consistant à définir et délimiter l'étude à partir des entretiens ou questionnaires établis à l'étape préparatoire.
- Expression des besoins et des évènements redoutés : énumération des besoins de sécurité de chacun des éléments essentiels.
- L'étude des menaces : étape ayant pour objectif de déterminer les menaces, puis les vulnérabilités associées à ces menaces, devant être couvertes par les objectifs de sécurité du système cible. On confronte ensuite les menaces spécifiques du système cible avec les besoins de sécurité établis précédemment.
- Identification des risques : détermination des risques, et définition des solutions permettant d'atteindre les objectifs de sécurité
- Détermination des exigences de sécurité : spécification des fonctionnalités attendues en matière de sécurité. Cela permet de démontrer la couverture des objectifs de sécurité par ces exigences de sécurité fonctionnelles ou mettre en évidence les éventuels risques résiduels. On doit enfin spécifier les exigences de sécurité d'assurance.
- Compléments : création d'un glossaire, d'une liste des acronymes utilisés dans l'étude et des documents de référence

- **Création de documents de synthèse** : EBIOS permet de réaliser différents livrables tels que des politiques de sécurité des systèmes d'information, des fiches d'expressions rationnelles des objectifs de sécurité (FEROS), des profils de protections, des cibles de sécurité… à partir des données issues d'une étude SSI.
- **Etude de cas :** Découvrir le logiciel à travers une étude de cas commentée.
- **Administration des bases de connaissances** : Le logiciel permet la création, la consultation et la personnalisation de bases de connaissances. Les bases de connaissances d'EBIOS présentent et décrivent des types d'entités, des contraintes, des vulnérabilités, des méthodes d'attaques, des objectifs de sécurité, des exigences de sécurité… Ces bases de connaissances sont ensuite utilisées par les études comme référence.
- **Administration système** : Administrer les utilisateurs. Cela correspond à la gestion des rôles et des utilisateurs (Authentification) : pour accéder à chaque fonctionnalité du logiciel, le logiciel peut demander un identifiant et un mot de passe.

Pour conclure, voici les principaux avantages du logiciel EBIOS :

Il est :

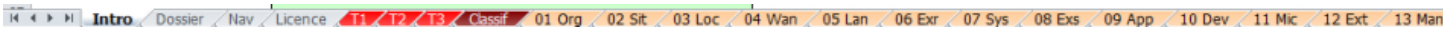
- Recommandé par la DCSSI (Direction centrale de la sécurité des systèmes d'information)
- Gratuit
- Compatible avec différents systèmes (Windows, Linux ou Solaris)
- Facile de prise en main (avec même un module d'auto-formation, une aide complète)
- Permet de rejoindre la communauté des utilisateurs EBIOS (experts…)
- Est sous licence libre (utilisable et adaptable par tous, sources et documents de conception fourni avec le logiciel) (conçu en UML et réalisé en Java et XML)
- Fidéle à la méthode
- Capable d'éditer les documents adaptés aux besoins

Le "logiciel" MEHARI

Contrairement au logiciel EBIOS qui nécessite une installation complète et qui utilise la technologie Adobe Air, l'outil proposé par MEHARI se présente comme un fichier de calcul Excel/OpenOffice permettant de couvrir tous les aspects de l'audit de sécurité. Ce dernier est accompagné d'un guide, le « Manuel de référence de la base de connaissances MEHARI 2010 » expliquant comment utiliser chaque feuille de calcul.
En effet, pour chacun des aspects de l'audit, on a une feuille de calcul associée.

Feuille de calcul de présentation de l'outil

On navigue donc entre ces feuilles afin de remplir toutes les données nécessaires à l'audit de sécurité.



Aperçu des onglets d'accès aux feuilles de calcul

L'onglet « nav » nous présente notamment la structure de la base de connaissances MEHARI qui fait partie de l'outil.

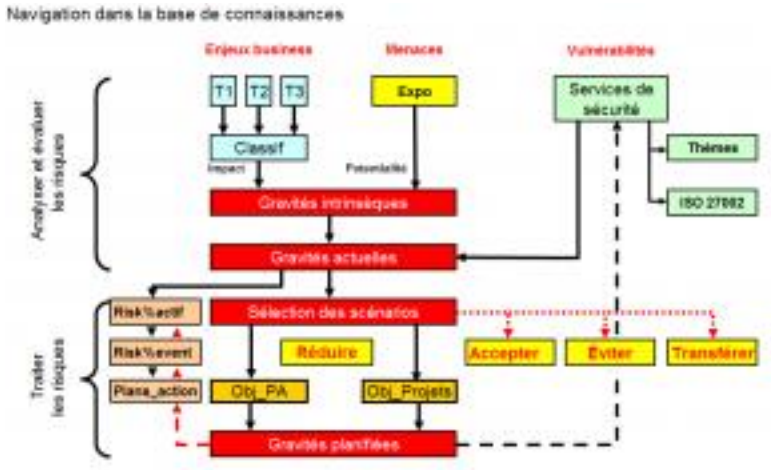


Schéma de l'organisation de la base des connaissances MEHARI

Analyse des enjeux et de la classification des actifs

Les premières données à entrer dans l'outil tiennent au remplissage des onglets T1, T2 et T3 qui permettent d'entrer les exigences de sécurité respectivement pour les types de données, les services et les processus de management issus de l'analyse des enjeux et du processus de la classification des actifs.
Les niveaux de classification des actifs à auditer sont ensuite référencés via l'onglet noté « classif », dans lequel on peut décider d'exclure certains actifs de l'audit et en conséquence de ne pas considérer les scénarios de risques associés à ces actifs.

Diagnostic des services de sécurité

On commence ensuite l'audit à proprement parler puisque les onglets suivants, numérotés de 1 à 14 constituent les questionnaires d'audit.
Les résultats de ces questionnaires sont synthétisés dans trois feuilles : les résultats des diagnostics par service, le récapitulatif par « thème » de sécurité et le score ISO, c'est-à-dire les résultats des diagnostics selon la classification ISO 27001/27002.

Evaluation des risques

Pour évaluer les risques, on commence par une évaluation de l'exposition naturelle aux risques, puis on envisage les différents scenarios à prendre en compte pour notre système.

Exemple de l'onglet Risk%actif

Via les onglets Risk%actif et Risk%event, on étudie la gravité des scénarios respectivement par type d'actif et par type d'évènement.

Préparation des plans d'actions

Après l'analyse, l'action ! Les onglets suivant permettent en effet de préparer les mesures à mettre en œuvre pour pallier aux manques de notre système. On a donc un récapitulatif des scénarios et des plans d'action que l'on peut mettre en place, puis, une fois la décision des plans à mettre en place prise, on revoit les objectifs de chaque plan et de chaque projet.

Exemples des vulnérabilités, grilles de paramétrage, etc.

Enfin, on a des onglets « annexes » permettant d'accéder à des conseils ou des exemples supplémentaires pour optimiser notre audit.

Le "logiciel" MEHARI permet d'établir le contexte (délimitation du périmètre et cadrage de l'étude), d'apprécier les risques (identification, estimation et comparaison) et de planifier et suivre le traitement des risques (mesures et risques résiduels). C'est un outil utile pour appliquer la méthode MEHARI, méthode reconnue de gestion des risques de sécurité des systèmes d'information (SSI).

Conclusion :

La sécurité informatique des systèmes d'information est un enjeu d'entreprise primordial actuellement. Nous avons vu ensemble qu'il existe de nombreux types d'attaques qui peuvent avoir des impacts très désastreux sur les finances et/ou l'image de marque des entreprises. Les entreprises se doivent de se mettre au norme en mettant en place des politiques de sécurité que cela soit au niveau physique, matérielle, humaine ou logicielle. Il en va de l'intégrité, de la confidentialité, disponibilité, non répudiation et imputation de données pouvant être très sensibles.
Pour cela, des méthodes de gestion des risques de sécurité des systèmes d'information existent. Les méthodes EBIOS, MEHARI ou encore FEROS sont les plus utilisées. Ces méthodes utilisent des outils puissant qu'il ne faut pas hésiter à utiliser.

Voici donc ce qu'il faut retenir (les **"Best Practices"**) en matière de plan de sécurité informatique de base :
1) Savoir quels sont les éléments les plus importants du système informatique
2) Protéger le réseau de l'entreprise
3) Ne pas se limiter aux serveurs "primordiaux" !
4) Prendre toutes les plateformes et tous les périphériques en compte :
5) Utiliser les bonnes protections
6) Centraliser l'administration
7) Être préparé à réagir dans l'urgence
8) Tester le plan d'action d'urgence et la stratégie de sécurité

Bibliographie :

- La sécurité de l'information - Stéphane Gill (2005)
- Site de l'Agence Nationale de la Sécurité Informatique (ANSI) tunisienne : http://www.ansi.tn/fr/audit/methodologies_audit.html
- http://www.bestpractices-si.fr
- Washington post
- Computer World UK : Site de nouvelles liées au monde de l'IT : http://www.computerworlduk.com
- Wikipédia
- Site de communication de Heartland Payment Systems sur leur piratage : http://www.2008breach.com
- Site de l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) française : www.ssi.gouv.fr
- Documentations et logiciel EBIOS
- Projet de sécurité des réseaux, Marc ROZENBERG, université d'Evry
- Site du clusif (**Clu**b de la **S**écurité de l'**I**nformation **F**rançais) : http://www.clusif.fr/

Annexe : Fiche détaillée des “Best Practices”

1) Quels sont les éléments les plus importants de votre système informatique ?

En effet, pour **avoir un concept de sécurité intéressant**, il est nécessaire de savoir**quels systèmes doivent être protégés en priorité**, ceux dont lesquels dépendent directement votre activité (si l’immobilisation du système immobilise l’entreprise) et quels systèmes auxiliaires y sont liés.

2) Protéger le réseau de l’entreprise :

Même si les systèmes informatiques de l’entreprise sont protégés individuellement, il est cependant souvent nécessaire de paramétrer le pare-feu (Firewall) afin de **permettre de manière sécurisée l’accès aux données de l’entreprise aux collaborateurs de terrain**, de façon fiable et rapide sans pour autant affaiblir la sécurité du système. Il s’agit donc de trouver un compromis entre la possibilité d’accès au données de l’entreprise de façon distante et de garder cet accès totalement sécurisé, comme un “réseau étendu” de l’entreprise.

3) Ne pas se limiter aux serveurs “primordiaux” !

Bien qu’il soit important de connaitre les points névralgiques de votre système/réseau informatique, **il ne faut pas se limiter à sécuriser les points les plus importants**. Les serveurs communiquant entre eux, ils doivent notamment TOUS être incorporés au concept de sécurité. Ainsi, si un malware infecte une machine, il peut ensuite se propager dans tout le réseau de l’entreprise, parfois y compris jusqu’aux points stratégiques de votre installation.

4) Prendre toutes les plateformes et tous les périphériques en compte :

Une idée reçue veut que seuls les systèmes Windows soient vulnérables aux attaques informatiques. FAUX ! **Toutes les plates-formes (Linux, Mac, Mobile, …) doivent inclus dans votre concept de sécurité.** De la même façon, avec l’importance toujours plus grande du sans-fil, les smartphones et les PC portables deviennent la majorité des machines utilisées et sont souvent moins sécurisés.

5) Quelles protections utiliser ?

La configuration minimale comprend au minimum **un scanner de virus** pour Windows, mais aussi pour Linux et Mac OS X, le cas échéant, **un pare-feu bien paramétré**, un**scan en temps réel des fichiers** de clés USB et des mails et des **accès contrôlés** pour les mobiles ou les smartphones. De plus, un **système de remise à zéro des informations du téléphone en cas de vol ou de perte** du mobile est en général mis en place, ainsi que la nécessité d’un code de déverrouillage sur le téléphone. Une autre fonction précieuse en matière de sécurité est le blocage des informations personnelles de l’abonné en cas de vol du smartphone et de retrait de

la carte SIM. Il est aussi extrêmement important de **tenir les logiciels à jour**, ce qui est malheureusement trop souvent oublié.

6) Centraliser l'administration :

Le concept de sécurité informatique se doit de prendre en compte tous les appareils et tous les serveurs et ces derniers doivent fonctionner ensemble. Il est donc très important que la protection de chacun soit gérée ou mise en place par **une équipe s'occupant de tous les aspects de la sécurité informatique** de votre entreprise. Un outil de suivi comportant une fonction de reporting est aussi nécessaire dès qu'il s'agit de gérer des parcs de machines conséquents.

7) Être préparé à réagir dans l'urgence :

En complément d'une stratégie de sécurité adaptée, un plan d'action d'urgence est nécessaire. Par une analyse des risques et des scénarios (comme cela est intégré aux démarches d'audit de sécurité sus-citées), **on peut se préparer aux cas les plus probables d'attaque ou de défaillance du système**.
Par exemple : En cas de soupçons justifiés d'un vol de données passé ou en cours dans l'entreprise, vous pouvez prendre les mesures suivantes :

- Informer la direction.
- Ne faire part à personne d'autre de vos soupçons.
- Contacter un professionnel des enquêtes informatiques.
- Ne tenter en aucun cas de mener votre propre enquête.
- Dresser la liste de tous les systèmes susceptibles d'être concernés.

8) Tester le plan d'action d'urgence et la stratégie de sécurité :

Bien entendu, il est toujours préférable et prévu que ces situations d'urgence ne se produisent pas. Mais tout comme un exercice anti-incendie, votre **plan d'action d'urgence informatique doit être testé**, les employés doivent être formés et il est mieux qu'une simulation ait lieu tous les six mois. L'évolution des menaces et la découvertes des failles étant toujours plus rapide, il est important que votre plan de sécurité soit dynamique et très régulièrement mis à jour.
Pour conclure, un système informatique est toujours faillible, car créé par l'Homme. Le principal est que la/les faille(s) soi(en)t inconnue(s) de tous, ou ne vaille pas la peine d'être exploitée. De la même façon, il est toujours possible que votre système soit perverti. Il est donc d'un extrême importance de **penser à sauvegarder régulièrement et dans différents endroits les données sensibles ou stratégiques.** "Mieux vaut prévenir que guérir", mais Mieux vaut aussi guérir que mourir : de l'utilité de se préparer toujours au pire.