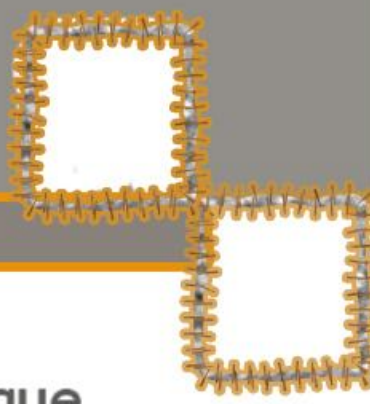
Informer, Communiquer, Manager

Concevoir la Sécurité Informatique en Entreprise



Penser des stratégies efficaces dans
la mise en oeuvre de la sécurité informatique
dans les organisations

Aman Vladimir

Avec le soutien et la collaboration de

A Propos de l'Auteur

Titulaire d'une Maîtrise en Criminologie Appliquée (MCA) à l'Université Félix Houphouët Boigny d'Abidjan, **AMAN VLADIMIR GNUAN** est *cybercriminologue* et passionné de Technologies de l'Information et de la Communication. Il nourrit un intérêt particulier pour l'univers de sécurité informatique et la criminalité liée au cyberespace, depuis ses premières années universitaires. Son intérêt pour la compréhension de la "criminalité et la sécurité publique" (délinquants, politique criminelle, Droit et procédure pénale, pénologie, sociologie du milieu carcéral, etc.), son goût prononcé pour l'Informatique et les TIC en général, ses premiers contacts professionnels avec le CERT Ivoirien, dénommé CI-CERT (Côte d'Ivoire - Computer Emergency Response Team), ont fortement motivés son orientation vers cette discipline.

Auteur du guide « Surfer en toute sécurité sur le web », blogueur, il officie en qualité de *Cybercriminologue* chargé de la communication/sensibilisation au sein de la Plateforme de Lutte Contre la Cybercriminalité (**PLCC**). Il est également consultant en cyberdroit et en stratégies de planification de la Sécurité des Systèmes d'informations auprès d'organisations privées.

Blog de l'auteur :

www.cybercrimactu.wordpress.com

Suivre l'auteur sur les réseaux sociaux :

vladimiraman@gmail.com

TABLES DES MATIERES

TROISIEME PARTIE :
RSSI, RM :LES NOUVEAUX METIERS DE LA SECURITE DES SYSTEMES D'INFORMATIONS

PREFACE

L'étude de la criminalité en général est restée longtemps un sujet mal compris ou plutôt mal apprécié. En effet, l'on a trop souvent réduit la lutte contre la criminalité à la création de lois répressives et au développement d'outils technologiques ou techniques de sécurité (antivol, barrières électriques, caméra de surveillance, etc.). Les travaux criminologiques ont pourtant montré que le passage à l'acte délictueux est la résultante d'une conjugaison de facteurs tant psychologiques, sociologiques, situationnels, que victimologiques.

Avec le développement des TIC et la rapide croissance de la communauté des internautes en Afrique, les problèmes liés à la sécurité dans le cyberespace ont acquis une importance plus que capitale pour les Gouvernements et aussi pour les dirigeants d'entreprises du secteur privé. En effet, le secteur privé reste le plus grand terrain de jeu de la cyberdélinquance, puisque générateur de ressources financières colossales. Mais comme dans bien des domaines, les entreprises Africaines se sont accaparées de technologies et méthodes de management, sans en maîtriser pleinement les contours.

Combien sont ces prestataires de services en ligne (e-commerce) et autres entreprises plongées dans un modèle de gestion numérisé, qui ne possèdent même pas les rudiments basiques de la sécurité informatique ?

Cet ouvrage se propose d'ouvrir le débat sur la conception de la sécurité des systèmes d'informations pour les entreprises du secteur privé et même des gouvernements. Loin d'être un recueil de « tutoriels » et de procédures techniques inopérantes, il aborde le concept de sécurité sous un angle plus large, afin d'ouvrir de réelles pistes de d'appréhension de la conception de la sécurité informatique en entreprise.

Complexes et nouvelles pour la plupart des Etats Africains, les TIC en général et Internet en particulier offrent un terrain nouveau d'investigation pour les spécialistes de domaines traditionnellement éloignés de la technique, à savoir : criminologues,

sociologues, juristes, commerciaux, etc. La cybersécurité reste un sujet encore très mal connu par l'opinion publique, du moins dans les pays Africains ; d'où la relative difficulté à apporter des éléments de réponses.

Le domaine de la sécurité informatique reste l'un des champs d'application les plus complexes de l'informatique. Les principes techniques énoncés dans l'ouvrage émanent d'une documentation sélective et de conseils pris auprès d'experts en sécurité Informatique exerçant au CI-CERT (Côte d'Ivoire Computer Emergency Response Team) et dans des entreprises indépendantes du secteur privé.

L'ouvrage « Concevoir la sécurité Informatique en entreprise », est composé de trois grandes parties, subdivisées en titres et sous-sections (1, 2, 3, etc.) et un bonus (thesaurus de la sécurité informatique) pour les lecteurs non techniciens. Il serait hasardeux et même prétentieux de donner quelques conseils ou autres indications purement techniques dans cet ouvrage, étant donné qu'il s'appuie sur des travaux et procédés déjà établis. Cet ouvrage doit être abordé, non pas comme un recueil de recettes magiques de sécurité informatique au sens technique du terme, mais plutôt comme un outil d'aide à la compréhension de la problématique de la sécurité informatique en entreprise.

Il s'adresse principalement aux personnes responsables à quelques niveaux que ce soit de la sécurité des systèmes d'information au sein des organisations. Il est conçu pour être accessible à toutes catégories de publics, quelque en soit la formation de base, car la sécurité reste une question de responsabilité partagée.

Aman Vadimir

INTRODUCTION

Internet, a-t-on coutume de le dire, est un espace virtuel transfrontalier offrant d'énormes opportunités, tant sur les plans économique, scientifique, que culturel. Comme toute société humaine, ce monde virtuel reste soumis aux principes fondamentaux régissant « le monde réel ». Les sociétés humaines ont de tout temps consentis des efforts colossaux quant à l'édition de règles et de principes directeurs, définissant le cadre général de leur fonctionnement. Ainsi, depuis les codes d'Ur-Nammu et d'Hammourabi, jusqu'aux différents CODES (pénal, civil, etc.) de l'époque contemporaine, l'on a toujours tenté d'encadrer autant que possible le fonctionnement de la société humaine. Mais, les crimes et actes allant à l'encontre des principes érigés ont toujours existé et constituent même dans un sens, le moteur de l'appareil législatif.

Si son apparition nous a grandement simplifié la vie, il est indiscutable que l'informatique nous a également apporté son corolaire de problèmes, inhérents à tous progrès scientifiques. De nos jours, presque tout est effectué par le biais de l'informatique : la sécurité, les transactions financières, la santé, l'administration (e-gouvernement), le divertissement, etc. Avec l'avènement des réseaux et du développement des TIC, la Sécurité des Systèmes d'Information (SSI) est devenue un sujet plus que capital, car de nos jours le système d'information (SI) est un élément absolument vital pour la plupart des entreprises.

Au delà de la stratégie commerciale et marketing proprement dite, ce qui permet aux entreprises d'atteindre leurs objectifs et de distancer leurs concurrents est de loin le SI[1], qui de ce point de vue apparait comme un outil vital pour celles-ci.

La mondialisation s'est avérée être un facteur déterminant dans le problème qui nous intéresse dans le cadre de cet ouvrage. En effet, la concurrence s'accroît davantage, ce qui potentialise les risques d'attaques de tous genres et offre plus de travail aux espions industriels et autres pirates informatiques.

[1] Système d'Informations

Puisque le système d'information est vital pour l'entreprise, tout ce qui menace sa sécurité est potentiellement « mortel[2] » pour l'entreprise. Maitriser les risques et prévoir autant que possible la probabilité d'occurrence d'incidents sur le système d'information, est devenu un enjeu déterminant pour la survie des entreprises. Toutefois, les règles et procédures à développer dans une entreprise doivent être conditionnées par les besoins, les objectifs, la culture de celle-ci et dans une vision plus large son environnement.

Si les entreprises semblent avoir compris la nécessité de sécuriser leurs systèmes d'informations, force est de constater que nombre d'entre elles ont adopté des conceptions inadéquates en s'alignant sur des modèles empruntés ça et là. Les mesures de prévention situationnelle, présentent certes des avantages indiscutables, mais peut-on pour autant s'en remettre exclusivement, face à une criminalité évolutive et toujours plus intelligente ?

De nombreux référentiels en matière de sécurité informatique ont été édités, mais l'on est tenté de se poser les questions suivantes : La sécurité Informatique peut-elle se résoudre à l'application de procédures techniques ? Les outils technologiques suffisent-ils pour garantir la sécurité des SI ? Peut-on parler de sécurité dans cet espace virtuel complexe qu'est Internet ? A-t-on connaissance des menaces internes et des implications psycho-sociales sur la sécurité ?

Telle est la problématique fondamentale de la conception de stratégies de sécurisation des systèmes d'informations en entreprise. C'est à toutes ces interrogations que nous essayerons d'ouvrir des pistes de réflexion, dans cet ouvrage.

[2] Par analogie le système d'informations est à l'entreprise, c'est qu'est que le cœur à l'Homme. Toute maladie affectant cet organe est potentiellement mortel.

PREMIERE PARTIE

FAIRE DE LA SECURITE INFORMATIQUE, QUELS IMPLICATIONS ?

1 DEFINITIONS

§1 LA SECURITE INFORMATIQUE

C'est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système informatique contre les menaces accidentelles ou intentionnelles auxquelles il peut être confronté. En d'autres mots, c'est l'ensemble des techniques qui assurent que les ressources du système d'information (matérielles ou logicielles) d'une organisation sont utilisées uniquement dans le cadre où il est prévu qu'elles le soient. Les exigences fondamentales de la sécurité Informatiques se résument à assurer:

- **La disponibilité** : L'information sur le système doit être toujours disponible aux personnes autorisées.
- **La confidentialité** : L'information sur le système ne doit être diffusée qu'aux personnes autorisées.
- **L'Intégrité** : L'information sur le système ne doit pouvoir être modifiée que par les personnes autorisées.

D’une manière générale, l’on pourrait retenir que la méthodologie de la sécurité informatique se définit comme suit :

- **Effectuer une analyse des risques**

Parce qu’il n’est possible de se protéger que contre les risques que l’on ne connait ! Ceci dit, il convient pour chaque entreprise d’évaluer les risques, c’est-à-dire les mesurer en fonction de la probabilité de leurs apparitions et de leurs effets possibles. Les entreprises ont tout intérêt à évaluer, quoique grossièrement ces risques et les moyens à mettre en œuvre, en fonction de leurs coûts. La notion de risque peut être appréhendée comme étant le produit d’un préjudice par la probabilité d’occurrence de celui-ci. La notion de risques est définie par les spécialistes selon l’équation suivante :

Risque = Préjudice x Probabilité d’occurrence

Cette formule sous-entend qu’un événement dont la probabilité est assez élevée mais dont il est possible de prévenir le préjudice qu’il peut causer, représente un risque **acceptable**. Il en va de même pour un événement à la gravité imparable (ex : effondrement d’un immeuble), mais à probabilité d’occurrence faible. Il va de soi que dans le premier cas, le risque ne devient acceptable que si les mesures de prévention contre le préjudice sont effectives et efficaces.

- **Etablir une politique de sécurité**

Une fois l’analyse des risques effectuée, la politique de sécurité est mise en place. Celle-ci a pour rôle de:

  - *Définir le cadre d'utilisation des ressources du système d'information;*
  - *Identifier les techniques de sécurisation à mettre en œuvre dans les différents services de l'organisation ;*
  - *Sensibiliser les utilisateurs à la sécurité informatique*

Mettre en œuvre des techniques de sécurisation

Ces techniques sont la réponse aux exigences fondamentales de la sécurité Informatique définies plus haut. Leur rôle est d'assurer la disponibilité, l'intégrité, la confidentialité et dans certains cas, la pérennité de l'information dans les systèmes d'information. Les techniques de sécurisation incluent notamment:

- *L'audit de vulnérabilités et Tests de pénétration (Pen-Test)*
- *La sécurisation des données: chiffrement, authentification, contrôle d'accès*
- *La sécurité du réseau: Pare-feu, IDS*
- *La surveillance des informations de sécurité*
- *L'éducation des utilisateurs*
- *Le plan de reprise des activités.*

§2 LE SYSTEME D'INFORMATION

Le système d'information est de nos jours, au cœur des stratégies commerciales, marketing et même de sécurité, de l'ensemble des entreprises. A l'ère de l'information, toute organisation se doit de consacrer une grande part de ses efforts, à la collecte, au traitement et à la diffusion de l'information, qu'elle-même génère du fait de son fonctionnement. Le système d'informations se distingue du système informatique, dans ce sens où ce dernier n'est qu'un composant du vaste ensemble que constitue **le système d'informations**.

Un système d'information est un ensemble organisé de ressources (qui peuvent être des données, des personnes, des activités ou des ressources matérielles en général), permettant de collecter, regrouper, classifier, traiter et diffuser l'information de façon adéquate en fonction des besoins et objectifs d'une organisation. Il est généralement délimité par un périmètre pouvant comprendre des sites, des locaux,

des acteurs (partenaires, clients, employés, etc.), des équipements, des processus, des services, des applications et des bases de données.

Au sein de l'entreprise, on peut distinguer plusieurs « sous-systèmes d'informations » qui mis ensemble, formeront le système d'information de l'entreprise. On peut distinguer par exemple, les systèmes de traitement de transactions (qui gèrent l'information concernant les transactions qui ont lieu dans une société), les systèmes d'information de gestion (pour résoudre les contraintes commerciales en général), les systèmes d'information décisionnelle (ils analysent les variables commerciales pour la prise de décisions), les systèmes d'information exécutive (pour les directeurs et les dirigeants), les systèmes d'automatisation de bureaux (applications qui aident au travail administratif) et les systèmes d'information spécialisés (qui émulent le comportement d'un expert d'un domaine concret).

Nous retiendrons que le système d'informations définit un ensemble d'interrelations entre :

- ***Des éléments*** : les logiciels, le matériel, les informations (composées de données, qui organisées et filtrées acquièrent le caractère d'aide à la décision).
- ***Des actions*** : ensemble de l'organisation et des procédures mises en place pour utiliser de façon optimale les éléments (logiciels, informations, etc.)
- ***Des individus*** : l'ensemble du personnel, des prestataires de services, des partenaires, etc. En somme les individus, c'est l'ensemble des acteurs qui interagiront par des actions sur les éléments.

§3 SYSTEME INFORMATIQUE

Un système informatique est un ensemble d'équipements (matériels et logiciels) destiné au traitement automatique de l'information. Il constitue la base sur laquelle repose un système d'information. En général, il est constitué de serveurs, routeurs, pare-feu, commutateurs, imprimantes, médias (câbles, air, etc.), points d'accès, stations de travail, systèmes d'exploitation, applications, bases de données, etc. En d'autres termes, il s'agit de tout le matériel informatique, qui est voué à traiter l'information.

Une information désigne un ensemble de données, transformées et filtrées, auxquelles l'on donne un sens par encodage, afin d'en permettre une compréhension et une exploitation facile. Elle constitue un puissant outil d'aide à la décision et a acquis avec le développement des TICs une valeur vitale pour l'entreprise. Le traitement de l'information consiste en :

- l'enregistrement de l'information (stockage dans des disques durs, serveurs, bases de données, etc.)
- la restitution de l'information (moniteurs, imprimantes, etc.)
- la modification de l'information
- la suppression de l'information

2 SECURITE INFORMATIQUE : RÊVE ACCESSIBLE ?

§1 PEUT-ON GARANTIR LA SECURITE EN INFORMATIQUE ?

La sécurité désigne en elle même une situation, un état dans lequel l'on n'est pas en danger. Il s'agit dans une vision plus large, d'un état de tranquillité d'esprit inspirée par la confiance, le sentiment de ne pas être menacé. Être en sécurité, c'est avoir la certitude d'être hors d'état d'être atteint par une menace quelconque. Appliquée au monde informatique, cette définition aurait du mal à s'appliquer, tant les menaces sont omniprésentes et multiformes. Hors mis les menaces extérieurs, l'utilisateur d'un système d'information constitue lui-même une menace pour l'intégrité de ce dernier.

Les problèmes de sécurité informatique peuvent de façon très générale être classés en deux grandes catégories :

- Ceux qui concernent la sécurité de l'ordinateur proprement dit, serveur ou poste de travail, de son système d'exploitation et des données qu'il abrite;
- Ceux qui découlent directement ou indirectement de l'essor des réseaux, ce qui multiplie la quantité et la gravité des menaces.

De plus, la résorption des vulnérabilités d'un système informatique, demeure un enjeu crucial pour les personnes dont les données sont gérées par un STAD

(système de traitement automatisé de données). Celle-ci repose sur un certain nombre de principes et de méthodes énumérés ci-dessous :

- Définir le périmètre de sécurité
- Définir les ressources publiques, ressources privées
- Identifier et authentifier : permettre l'accès aux personnes selon leurs importance et les informations auxquelles ils souhaitent accéder
- Empêcher les intrusions : Installer des pare-feu, filtrer les communications réseaux, établir des zones dématérialisées dans le réseau (DMZ), installer des systèmes de détection d'intrusion (IDS), installer des systèmes de prévention d'intrusion (IPS)
- Etablir une politique de défense en profondeur 3: limiter les conséquences d'une attaque réussie. L'intégration du concept de défense en profondeur dans les techniques de sécurisation des systèmes d'informations, traduit l'acceptation de ce que la sécurité ne peut être totalement garantie. La conception moderne de la protection des systèmes et des réseaux s'appuie sur la notion de défense en profondeur, par opposition à la défense rigide, où l'on mise tout sur l'efficacité absolue d'un dispositif de sécurité unique.

Avec le développement des réseaux et d'Internet, l'information acquiert une place centrale dans la stratégie des entreprises. En effet, l'information devient un véritable trésor, voire le cœur de l'entreprise étant donné que tout est dématérialisé.
Pour l'entreprise, la sécurité informatique répond à deux grandes exigences : Protéger les informations publiques et protéger les informations privées.

[3] La multiplication des vulnérabilités, la généralisation des ordinateurs portables qui se déplacent hors du réseau de l'entreprise, l'usage de logiciels novateurs (code mobile, Peer to Peer (P2P), sites interactifs, téléphonie et visioconférence sur IP) et d'autres innovations, ont anéanti la notion de « périmètre de sécurité » de l'entreprise. Ceci oblige le responsable SSI à considérer que la menace est partout et peut se manifester n'importe où. Il faut continuer d'essayer d'empêcher les intrusions dans le SI de l'entreprise, mais le succès de la prévention ne peut plus être garanti, raison pour laquelle il faut se préparer à limiter les conséquences d'une attaque réussie, qui se produira forcément un jour.

Protéger les informations publiques

Cette catégorie d'informations est librement diffusée sur Internet, car elle ne constitue pas une ressource à protéger. Cela dépend toutefois de l'activité exercée par l'entreprise. Il s'agit par exemple des nouvelles offres, des achats en ligne, de la mise à jour de systèmes, de logiciels, des coordonnées du service client, du service technique, des contacts du webmaster pour le site Internet, etc. Tout type d'information qui ne peut mettre en danger ni l'entreprise, ni ses partenaires commerciaux, ni ses sous-traitants ou ses clients. Il s'agit de toutes informations qui ne sont pas considérées comme sensibles pour l'entreprise, en tenant de la politique Interne et des objectifs de l'entreprise.

Protéger les informations privées

Il s'agit des informations transmises au sein de l'entreprise par l'Intranet, les emails internes ou par courrier interne. Elles concernent par exemple les règles, les procédures et les organigrammes de l'entreprise, les publications d'annuaires, le nom des systèmes internes, les versions de logiciel ou matériel utilisé, etc. Afin de renforcer la sécurité de l'entreprise, il est plus que nécessaire que les employés aient des outils pour se défendre contre les attaques et qu'ils sachent aussi contre-attaquer en cas d'attaque ou d'incident informatique avéré.

§2 LE PARADOXE DU CONCEPT DE "SECURITE INFORMATIQUE"

Les potentialités énormes qu'offrent Internet pour le développement des entreprises de tous les secteurs d'activités n'est plus à démontrer. Les caractéristiques spécifiques d'Internet, qui présente la particularité d'être un espace transfrontalier détenu et contrôlé à la fois par personne et par tout le monde, en font un pourvoyeur d'opportunités d'affaires illimitées. De nombreuses entreprises grandes ou petites, ont très bien compris cet d'état de fait et ont donc construit leurs modèles économiques sur cette base. C'est le cas par exemple d'entreprises interconnectées avec leurs représentations dans différents pays du monde. Dans cette configuration, fournisseurs, partenaires logistiques, clients, travailleurs, etc. se trouvent bien sur le même système d'information, sans être forcément sur le même espace géographique. En effet, tous les acteurs de la chaîne partage le même environnement réseau mis en œuvre dans le cadre des activités professionnelles, sans pour autant se trouver sur le même espace géographique. De plus, les possibilités d'interconnexion des différents segments d'une entreprise disséminée à travers le monde, s'en voient décuplées avec le développement incessant de technologies toujours plus innovantes (fibre optique, cloud, etc.). Indiscutablement, de telles architectures d'entreprise n'auraient jamais pu être possibles sans Internet.

En somme, Internet ouvre à des coûts significativement réduits sur le monde extérieur et attire des opportunités énormes diversifiées, favorisant ainsi la genèse et le développement d'idées et de concepts novateurs en termes d'affaire.

Cependant, tout ceci crée aussi de nouvelles menaces auxquelles il faudra faire face en même temps que l'on étend son champ d'activité via le web. En effet, en opérant dans un environnement aussi « ouvert » qu'Internet, les entreprises se trouvent exposées à des attaques qui n'auraient pu avoir lieu dans un environnement complètement fermé. Ainsi, les attaques de type [4]DoS, [5]DDoS, Botnet, Backdoors,

[4] Denial of services : dénis de service

IP Spoofing, Flooding, etc, dont le fondement repose sur une attaque généralement perpétrée depuis l'extérieur, n'auraient simplement jamais existées. De l'autre coté, elles développent des opportunités d'affaire qui auraient été inexploitables aux mêmes coûts dans un environnement fermé.

D'un point de vue marketing et commercial, les entreprises et organisations sont contraintes, sous l'effet de la concurrence et de la diversité des marchés, de développer des stratégies nouvelles en proposant des services à valeur ajoutée, pour booster leurs chiffres d'affaires. Ceci dit, Internet et les TIC apparaissent de loin comme le canal privilégié pour cette « *nouvelle guerre des marchés* ».

En résumé, à l'heure des TIC et du web 2.0, la tendance est plutôt vers l'ouverture, ce qui implique nécessairement une évolution des menaces cybercriminelles, d'où la nécessité de mettre un accent particulier sur les politiques de sécurité Informatique.

[5] Distributed deny of services : Déni de service distribué, (voir Thesaurus de la Sécurité Informatique)

3 RISQUES ET ENJEUX DE LA SECURITE INFORMATIQUE EN ENTREPRISE

§1 LES RISQUES

Un risque permet de mesurer les possibilités de l'occurrence d'un événement, associé à une situation ou une activité. De l'autre coté, un enjeu est grossièrement ce que l'on peut gagner ou perdre en posant un acte. Dans le cas de la sécurité informatique en entreprise, il s'agit plutôt de ce que l'on peut perdre, en l'absence de moyens adéquat de sécurisation. Lorsque l'on évoque les risques susceptibles d'engendrer un *incident informatique* sur le Système d'Information d'une entreprise, on distingue deux grandes catégories :

- **Les risques physiques**
- **Les risques logiques**

1. Les risques physiques

Il s'agit de toutes les atteintes physiques directes dont peut être victime un système d'informations au cours de son cycle de vie. On les appelle également risques matériels, parce qu'ils ont trait à l'intégrité du matériel. Il s'agit entre autres d'événements tels que:

- Incendies, explosion, effondrement
- Dommages électriques, foudre
- Tempêtes, inondations, événements naturels
- Bris de machines, vol, actes de vandalisme
- Défaillance matérielle

Ces risques physiques peuvent être d'origine accidentelle ou malveillante et les conséquences sont aisément identifiables. Ces incidents détériorent les ressources matérielles du système d'information et peuvent avoir un impact direct sur les actifs informationnels que contiennent les systèmes informatiques.

Les risques physiques constituent dans la conception traditionnelle de la sécurité, les premières sources d'inquiétude des responsables d'entreprise en termes de sécurité, même si en pratique, ils ne représentent qu'un faible pourcentage des sinistres informatiques enregistrés en entreprise.

2. Les risques logiques

Avec le développement fulgurant de l'informatique distribuée[6] par opposition à l'informatique centralisée, les données et les applications ont acquis une importance plus grande. En effet, l'on assiste à une migration progressive de la valeur du matériel vers la valeur des données et des applications. Le développement du [7]Cloud Computing est l'une des illustrations les plus expressives de cette tendance. La question principale est de savoir comment évaluer et analyser la valeur de ce qui n'est pas physique, donc immatériel c'est-à-dire la **donnée**.

C'est pour répondre à cette question que sont apparues les notions d'*accident*, d'*erreur* et de *malveillance*, directement issues des méthodes d'analyse des risques développées ces dernières années.

[6] L'informatique distribuée correspond à la structure de la société humaine, en réseau, où chacun est différent et avance à son rythme
[7] Informatique dans les nuages

L'accident : Il s'agit là d'un événement perturbant les données ou les flux de données, en l'absence de dommages physiques aux équipements (altération physique du matériel).

L'erreur : Il peut s'agir d'une erreur de conception, de programmation, de paramétrage ou de manipulation des données et de leurs supports. L'erreur désigne des préjudices consécutifs à l'intervention humaine dans le processus de traitement automatisé des données. Elles constituent les risques les plus fréquents dans le cycle de vie d'un système d'information en entreprise.

La malveillance : Il s'agit de tous actes traduisant la volonté manifeste de son auteur de faire usage, sans autorisation d'un système d'information, avec des intentions préjudiciables. Le virus informatique et l'acte de malveillance le plus médiatisé, quoiqu'il en existe une très grande diversité (Botnet, Chevaux de Troie, etc.).

De nos jours, les enjeux énormes mis en lumière par l'intelligence économique, ont modifié le statut de la donnée informatique pour en faire de « l'information ». La valeur de l'information n'est plus statique comme c'était le cas des années en arrière, mais elle fluctue au gré de sa nécessité, son environnement et bien d'autres facteurs. Ceci dit, une information peut représenter un enjeu stratégique plus ou moins important dans des délais très courts en fonction de divers facteurs environnementaux. La liste des risques logiques courus par une entreprise est énorme, mais nous nous limiterons à dresser dans le cadre de cet ouvrage, une liste non exhaustive de ces risques que l'on a regroupé en quatre catégories :

Vol d'informations : Avec Internet, le vol s'en trouve dématérialisé, étant donné que l'objet dérobé est une valeur virtuelle, voire abstraite. Il s'agit pour l'entreprise de risques tels que : espionnage industriel, vol des listes des clients, vol d'informations comportant des données personnelles de clients ou du personnel, vol des plans ou les recettes des productions, vol de la comptabilité.

Usurpation d'identité : Utilisation du compte d'un client ou d'un partenaire, utilisation des identifiants d'une personne de l'entreprise à des fins malveillantes, etc. Une usurpation d'identité peut avoir des conséquences énormes sur l'image de marque d'une entreprise.

Intrusions et utilisation des ressources systèmes : Il s'agit de : Utilisation des ressources de l'entreprise afin lancer des attaques informatiques (machines zombies, botnet, etc.), corruption de base de données, etc.

Mise hors service des systèmes et des ressources informatiques : Surcharge du site web ou du serveur de messagerie de l'entreprise (DoS, DDoS, mail bombing), virus, attaque du réseau de l'entreprise.

Par exemple, une personne mal intentionnée inonder le serveur d'une entreprise de requêtes, jusqu'à ce que celui-ci ne soit en mesures de répondre aux requêtes et s'arrête de fonctionner ; rendant ainsi indisponible le Site web de l'entreprise pendant de longues heures.

§2 LES ENJEUX

Les risques énumérés plus haut peuvent avoir un impact direct ou indirect sur l'entreprise par l'entremise des différents utilisateurs du Système d'Information que sont ses clients, ses employés ou ses partenaires d'affaires.

En considérant que l'information est la résultante de l'utilisation du matériel, des logiciels et des données contenues dans le SI, la notion d'impact est divisée en quatre familles :

- Impact sur la disponibilité de l'information
- Impact sur l'intégrité de l'information

- Impact sur la confidentialité de l'information
- Impact sur la preuve ou la traçabilité

Les conséquences d'incidents informatiques peuvent être énormes et avoir une répercussion très significative sur l'ensemble de l'activité d'une entreprise. On les classe généralement en quatre catégories, en tenant compte des quatre familles d'impact susmentionnées.

1. Sur le plan financier

La perte de valeur et de biens, Coût d'immobilisation de l'entreprise entrainant un ralentissement des activités en raison de pannes informatiques ou électroniques, perte de production, etc.

Coût du temps passé : recherche de l'origine de l'attaque, réparation, restauration des données, ressaisies des données perdues, réinstallation des programmes informatiques, reconfiguration des serveurs

Coûts techniques : remplacement d'un disque dur et de tout autres matériels informatiques, honoraires d'experts pour la résolution de problèmes complexes, hausse des tarifs d'assurances, etc.

2. Atteinte à l'image

Dans le cas d'un incident informatique, l'une des conséquences les plus difficiles à évaluer reste le ressentiment que peuvent avoir les clients, vis-à-vis de la confiance qu'inspire les produits et services. La dégradation de l'image de marque et perte de la crédibilité sont des conséquences absolument dommageables pour l'entreprise, surtout en l'absence d'une politique de gestion de communication de crise efficace.

3. Sur le plan humain

Sur le plan humain, les conséquences d'incidents informatiques peuvent induire un risque vital pour l'employé. Exemple d'un employé qui en arrive à se donner la mort, culpabilisant du fait que l'infection du réseau informatique et les conséquences qui s'en soient suivies, soit survenue du fait de son imprudence ou de sa négligence. De tels dénouements dramatiques en entreprise, peuvent entrainer une réaction à la chaîne qui se traduirait par une désorganisation du personnel, impact psychologique très fort sur les collègues, baisse de la performance, etc.

Les conséquences sur le plan humain peuvent être faciles à contenir, à travers une politique de suivi social et d'accompagnement des employés.

4. Sur le plan juridique

En cas d'incident informatique, la responsabilité civile et pénale de l'entreprise vis-à-vis d'autrui, des contractants, des clients, des partenaires, des autorités, etc., peut être engagée et avoir des répercussions très lourdes sur la vie de l'entreprise (paiement d'amendes, retrait d'autorisations, agréments, etc.). Des législations plus avancées en matières de cybersécurité prévoient des sanctions très lourdes pour des entreprises dont le système non ou mal sécurisé cause un préjudice aux utilisateurs de ses services (clients de banque par exemple).

4 SECURITE INFORMATIQUE : PLUS QU'UN CONCEPT STRATEGIQUE, UNE QUESTION DE GOUVERNANCE

La notion de gouvernance d'entreprise est un concept récent qui est apparu dans le début des années 1990. La gouvernance d'entreprise peut être définie comme l'ensemble des règles permettant aux actionnaires ou partenaires de s'assurer que les entreprises dont ils détiennent des parts ou dans lesquelles ils ont un intérêt particulier, sont dirigées en conformité avec les visions et objectifs fixés par consensus.

Par exemple, l'intérêt de la nation est fortement engagé en ce qui concerne l'impact de la cybercriminalité sur les entreprises publiques et même privées des secteurs stratégiques et critiques (énergie, santé, banque, etc.) au plan national. De ce point de vue, l'Etat apparait comme un partenaire de premier ordre des autres acteurs du secteur privé, en ce qui concerne la cybersécurité nationale.

Si les systèmes juridiques, les cadres institutionnels, les habitudes et les cultures diffèrent selon les pays, l'une des questions fondamentales à laquelle ils sont tous confrontés est de savoir comment faire en sorte que les dirigeants des entreprises privées, agissent au mieux des intérêts des actionnaires dont l'Etat figure au premier rang. A ce sujet, les pays dit industrialisés ont compris la nécessité de « contrôler »

les dirigeants du secteur privé, en mettant en œuvre des mesures réglementaires et organisationnelles en matière d'encadrement de la sécurité dans le secteur des TIC.

§1 LOIS ET CONVENTIONS

1. La loi Sarbanes-Oxley

La loi Sarbanes-Oxley, des noms respectifs des deux sénateurs Paul Sarbanes et Michael G. Oxley, a été adoptée par le congrès Américain en Juillet 2002. Cette loi, aussi dénommée Public Company Accounting Reform and Investor Protection Act of 2002 ou plus simplement SOX ou Sarbox, est la réponse aux multiples scandales comptables et financiers : Enron, Tyco International ou encore WorldCom. L'application de cette loi entre en vigueur pour toutes les entreprises Américaines cotées au NASDAQ ainsi que leurs filiales à l'étranger. Chacune d'entre elle doit certifier ses comptes auprès de la Securities and Exchanges Commission (SEC), l'organisme de régulation des marchés financiers Américains. Cette loi prend en compte les aspects suivants :

- ***La gestion des mots de passe***

- Le niveau de sécurité des mots de passe ;
- La vérification du changement des mots de passe tous les six (06) mois
- L'étude des notes délivrées par le responsable sécurité aux employés sur la politique des choix de mots de passe
- Un exemple concret de test consisterait à évaluer la sécurité des mots de passe de 30 utilisateurs, et à identifier la proportion de mots de passe faibles.

- ***L'étude de réseau informatique***

- Vérification de l'authentification des accès VPN ;
- Protection du réseau interne par 2 niveaux de pare-feux ;

- Contrôle et journalisation des accès à Internet ;
- Signature d'une charte de bon usage d'Internet ;
- Authentification des utilisateurs pour accéder à Internet ;
- Révocation des certificats lors du départ des collaborateurs

❖ ***La gestion des Antivirus et des correctifs***

- Effectuer un filtrage efficace sur les serveurs de mails afin d'éviter toute propagation de vers et de fichiers malicieux sur le réseau interne.
- Analyse virale de tous les messages qui transitent par le serveur SMTP.
- Un contrôle des mises à jour doit être effectué chaque mois par un responsable informatique.

❖ ***Plan de reprise en cas de désastres***

- Cet aspect a pour objectif d'évaluer les capacités de l'entreprise à faire face à un incident grave.
- Sauvegarde des serveurs principaux
- Externalisation des supports de sauvegarde.
- Rédaction d'un document de procédure de restauration pour chaque serveur.

❖ ***La sécurité des applications ERP***[8]

La sécurité des ERP constitue un point clé de la loi Sarbanes-Oxley. Elle prévoit entre autres :

- Contrôles stricts de l'accès : attribution de droits aux utilisateurs des différentes ressources.
- Utilisation de mots de passe longs et une authentification établie toutes les 15 minutes lorsque l'application n'est pas utilisée.
- Accessibilité des données seulement aux utilisateurs autorisés.

[8] ERP : Enterprise Resource Planning (ERP) ou Progiciel de Gestion Intégré (PGI) est un logiciel qui permet de gérer l'ensemble des processus d'une entreprise, en intégrant toutes les fonctions de cette dernière comme la gestion des ressources humaines, la gestion comptable et financière, l'aide à la décision, mais aussi la vente, la distribution, l'approvisionnement, le commerce électronique.

❖ *La gestion des ordinateurs portables*

Il est nécessaire de prendre des mesures précises, afin d'éviter toute perte et vol de données ou l'infection du réseau par des virus.

- Présence d'un pare-feu personnel sur chaque ordinateur portable
- Activation par défaut de l'exécution des mises à jour des anti-virus, des logiciels et du système d'exploitation

❖ *Les sauvegardes*

- Sauvegarde des serveurs et des postes sensibles.
- Spécification de la durée de rétention des sauvegardes en fonction de chaque entreprise.
- Réalisation de tests de restauration tous les quatre à six mois.

❖ *La journalisation & Audits*

- Vérification de l'existence des fichiers de logs des serveurs mails, des navigateurs internet, des accès VPN?
- Traçabilité des accès aux applications financières et ressources humaines
- Sauvegardes des e-mails conservées durant 1 mois minimum (destinataire, l'envoyeur, le sujet, la date et l'heure et l'IP)

❖ *La gestion des vulnérabilités*

- Réaliser des tests de vulnérabilités chaque mois sur les serveurs critiques, assortis de rapports écrits par les responsables de la sécurité.

❖ *La sécurité physique*

- Réglementer de manière stricte l'accès aux bâtiments et aux ressources informatiques.
- Contrôle et restriction des accès aux différentes zones de l'entreprise via un système de contrôle.
- Passage obligatoire des visiteurs par l'accueil pour être enregistrés.

- Protection des salles des serveurs informatiques par un lecteur de badges

❖ ***La sécurité des bâtiments***

- Protéger les bâtiments contre les incendies et sécuriser les flux afin d'éviter les vols de données.
- Affichage du plan d'évacuation à chaque étage.
- Réalisation d'un test d'évacuation d'urgence une fois par an.
- Présence d'alarmes incendies ainsi que de portes anti-feu dans chaque bâtiment

2. Les accords de Bâle

Ils ont pour objectif de contrôler l'ensemble des risques auxquels les établissements bancaires/financiers sont soumis. Ces accords spécifiques aux établissements financiers Bâle I, II, III, en raison de leur grande maturité en matière de gestion des risques, se rapprochent ainsi de réglementations plus génériques comme la loi Sarbanes-Oxley précitée. La dernière version de ces accords en cours d'application est Bâle II. Ces accords ont pour objectif de mieux appréhender les risques bancaires et permettre une gestion plus fine des risques en phase avec la réalité économique.

Ils s'appuient sur trois piliers essentiels :

- Exigence de fonds propres
- Surveillance de la gestion des fonds propres
- Transparence

3. Le standard PCI DSS[9]

Ce standard est destiné aux plus importantes entreprises de carte de débit et crédit. Il s'agit en réalité d'un guide de 12 règlements qui aident les entreprises émettrices de cartes de paiement à protéger leurs données et à prévenir les fraudes. Ces douze règlements sont :

- Installer et gérer une configuration de pare-feu afin de protéger les données des titulaires de carte ;
- Ne pas utiliser les paramètres par défaut du fournisseur pour les mots de passe et les autres paramètres de sécurité de système ;
- Protéger les données des titulaires de cartes stockées ;
- Crypter la transmission des données des titulaires de carte sur les réseaux publics ouverts ;
- Utiliser et mettre à jour régulièrement un logiciel antivirus ;
- Développer et gérer des applications et systèmes sécurisés ;
- Limiter l'accès aux données des porteurs de carte aux cas de nécessité professionnelle absolue ;
- Attribuer une identité d'utilisateur unique à chaque personne disposant d'un accès informatique ;
- Limiter l'accès physique aux données des titulaires de carte ;
- Suivre et surveiller tous les accès aux ressources du réseau et aux données des titulaires de carte ;
- Tester régulièrement les systèmes et procédures de sécurité ;
- Disposer d'une politique régissant la sécurité de l'information.

[9] PCI DSS (Payment Card Industry Data Security Standard) est un standard de sécurité des données, pour les industries de carte de paiement créé par le comité PCI SSC.

4. La norme ISO 27001

La série **ISO 27000** est déclinée en plusieurs sous-normes indicées, thématiques et sectorielles dédiées à la sécurité de l'information. Il traite aussi bien de la gestion des risques que du pilotage de la fonction (indicateurs et tableaux de bord).

Thématique de l'ensemble ISO 27000, **ISO 27001** est une norme d'origine britannique dédiée au système de management de la sécurité de l'information. La norme ISO 27001 est orientée processus et propose en toute logique une démarche d'amélioration continue de type PDCA et constitue le standard principal décrivant les exigences d'un système de pilotage de la sécurité des informations. Le PDCA ou **roue de deming** propose 4 temps : « Plan- Do- Check -Act » ou Planification, Déploiement, Contrôle et Action.

i. **Planification** (Plan): ***Etablir le SMSI*** (Système de Management de la Sécurité de l'Information) :

La planification consiste à élaborer la politique de sécurité des SI, déterminer le périmètre d'intervention, définir les objectifs, analyser et maîtriser les risques. L'entreprise doit respecter les points de contrôles suivants :

- Définir le champ détaillé d'application du SMSI (processus métiers, organisation, location, biens, technologies) ;
- Définir la politique du SMSI ;
- Définir l'approche d'évaluation des risques (méthode, critère d'acceptation, etc.) ;
- Identifier les risques (biens traités, menaces, vulnérabilités potentielles, impacts) ;
- Analyser et évaluer les risques (impact métier, probabilité, gravité) ;
- Définir la stratégie de traitement des risques (transfert, accepte, etc.) ;
- Définir les mesures (objectifs, points de contrôle) de limitation des risques;

- Obtenir l'accord du management sur la stratégie de traitement des risques;
- Obtenir l'accord du management pour implémenter le SMSI ;
- Formaliser la stratégie de traitement des risques (choix des mesures à mettre en œuvre, liste des mesures déjà appliquées, justification de l'élimination de points de contrôle).

ii. Déploiement (Do): Mettre en place et exploiter le SMSI

Il s'agit ici d'établir le plan et déploiement des mesures de sécurité, élaboration et application des procédures spécifiques, sensibilisation et formation, sélection des indicateurs et réalisation des tableaux de bord sécurité. L'entreprise doit respecter les points de contrôles suivants:

- Définir un plan d'actions de traitement des risques (mesures de protection, ressources, responsabilités, priorité, etc.) ;
- Organiser le déploiement du plan d'actions de traitement des risques ;
- Déployer les points de contrôle et les mesures de protection ;
- Définir la stratégie de suivi et de mesure de l'efficacité des actions
- Déployer un programme de formation et de sensibilisation ;
- Piloter et gérer les aspects opérationnels du SMSI ;
- Mettre en œuvre des procédures et des moyens de détection et de traitement des incidents.
- Réévaluer régulièrement les risques ;
- Effectuer régulièrement des audits du SMSI ;
- Organiser le suivi du SMSI au niveau du Management (Direction Générale) ;
- Adapter et mettre à jour le plan d'actions sécurité (prendre en compte les indicateurs de suivi d'efficacité) ;
- Enregistrer les actions et les évènements qui peuvent avoir un impact sur l'efficacité du SMSI.

iii. **Contrôle (Check):** Contrôler et évaluer le SMSI

A ce niveau, il s'agit de réaliser des audits et contrôles internes et aussi des revues. L'entreprise doit respecter les points de contrôles suivants :

a) Mettre en œuvre les procédures et les moyens de suivi (détection d'erreurs, suivi des incidents, des tentatives d'exploitation de failles, contrôle des performances humaines et technologiques, etc.) ;
b) Organiser le suivi de l'efficacité du SMSI, en prenant en compte les résultats d'audit, les relevés d'incidents, les mesures d'efficacité, les suggestions et avis des intervenants dans le SMSI, etc.)
c) Mesurer et contrôler l'efficacité des mesures déployées ;

iv. **Action (Act):** Soutenir et améliorer le SMSI

C'est la dernière étape du processus PCDA, qui consiste à appliquer les actions correctives, identifier des voies d'amélioration et réaliser le bouclage. L'entreprise doit respecter les points de contrôles suivants :

a) Implémenter les modifications identifiées dans le SMSI ;
b) Prendre des mesures correctives et préventives (prendre en compte les retours d'expérience internes ou externes) ;
c) Communiquer sur les mesures et les adaptions du SMSI aux personnes impliquées ;
d) Vérifier que les correctifs/modifications répondent aux objectifs fixés.

5. La norme ISO 27002

La norme ISO/CEI 27002 est composée de onze sections principales, qui couvrent le management de la sécurité aussi bien dans ses aspects stratégiques que dans ses aspects opérationnels. Chaque section constitue un chapitre de la norme :

- Chapitre 1 : Politique de sécurité
- Chapitre 2 : Organisation de la sécurité de l'information
- Chapitre 3 : Gestion des biens
- Chapitre 4 : Sécurité liée aux ressources humaines
- Chapitre 5 : Sécurité physique et environnementale
- Chapitre 6 : Gestion des communications et de l'exploitation
- Chapitre 7 : Contrôle d'accès
- Chapitre 8 : Acquisition, développement et maintenance des systèmes d'information
- Chapitre 9 : Gestion des incidents liés à la sécurité de l'information
- Chapitre 10 : Gestion de la continuité d'activité
- Chapitre 11 : Conformité légale et réglementaire

Même si les seulement deux normes ont été présentées dans le cette section, il faut savoir que l'ensemble ISO 27000 est constitué de 12 thématiques.

Intitulé	Statut	Date publication/révision	Domaine
ISO/CEI 27000	publié	2009	Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire
ISO/CEI 27001	publié	2013	Système de Gestion de la Sécurité de l'Information (ISMS) — Exigences
ISO/CEI 27002	publié	2013	Code de bonnes pratiques pour la gestion de la sécurité de l'information (anciennement ISO/CEI 17799)
ISO/CEI 27003	publié		Système de Gestion de la Sécurité de l'Information (ISMS) — Guide d'implémentation

ISO/CEI 27004	publié		Mesure de l'efficacité la sécurité de l'information mise en œuvre
ISO/CEI 27005	publié	2009	Gestion du risque en sécurité de l'information
ISO/CEI 27006	publié	2008	Exigences pour les organismes réalisant l'audit et la certification de Systèmes de Gestion de la Sécurité de l'Information (ISMS)
ISO/CEI 27007	publié		Guide pour l'audit de Systèmes de Gestion de la Sécurité de l'Information (ISMS)
ISO/CEI 27008	publié		Lignes directrices de vérification en matière de mesures de sécurité concernant ISO 27002
ISO/CEI 27011	publié	2008	Guide pour l'implémentation de ISO/CEI 27002 dans l'industrie des télécommunications
ISO/CEI 27031	publié	2012	Code de bonnes pratiques en matière de Technologies de l'information – Techniques de sécurité – Lignes directrices pour mise en état des technologies de la communication et de l'information pour continuité des affaires
ISO/CEI 27799			Informatique de santé - Gestion de la sécurité de l'information relative à la santé en utilisant l'ISO/CEI 27002

Tableau 1: Tableau récapitulatif des normes de la série ISO 27000

Projet	Domaine
ISO/CEI 27010	Gestion de la communication inter secteur
ISO/CEI 27031	Continuité d'activité
ISO/CEI 27032	Cyber sécurité
ISO/CEI 27033	Sécurité réseau
ISO/CEI 27034	Sécurité des applications
ISO/CEI 27035	Gestion des incidents
ISO/CEI 27036	Audit des mesures de sécurité du SMSI
ISO/CEI 27037	Gestion des preuves numériques

Tableau 2: Tableau récapitulatif des normes ISO en projet

§2 LES METHODES DE SECURITE

1. EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité)

Cette méthode fait partie d'une série de guides méthodologiques publiés par la direction centrale de la sécurité des systèmes d'information (DCSSI)10 du ministère de la défense française. Elle est notamment préconisée dans l'administration française et dans les entreprises. Cette méthode, créée en 1995, se compose de cinq guides (Introduction, Démarche, Techniques, Outillages pour l'appréciation des risques et Outillages pour le traitement des risques) et d'un logiciel support permettant la mise en œuvre de la méthode. Le logiciel a accès à une base de connaissances donnant accès à la description d'un ensemble de vulnérabilités

[10] L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a été créée par le décret n° 2009-834 du 7 juillet 2009 (*Journal officiel* du 8 juillet 2009), sous la forme d'un service à compétence nationale. Elle est rattachée au Secrétaire général de la défense et de la sécurité nationale (SGDSN), autorité chargé d'assister le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale.

spécifiques, de contraintes de sécurité, de méthodes d'attaques. EBIOS appréhende les risques de sécurité en tenant compte des trois blocs interdépendants des concepts de gestion présentés en amont. La méthode travaille par construction du risque, adoptant une prise en compte du contexte de l'organisation cible, en privilégiant le périmètre du SI, les éléments essentiels, les fonctions et les informations (correspondant aux ressources business) et enfin les entités (ressources système). La seconde phase de la méthode permet de dégager les besoins via une grille des services souhaités de sécurité. Le risque adapté à l'organisation est ainsi construit et renforcé par la prise en compte relative des vulnérabilités et des menaces s'appliquant sur les ressources jugées critiques.

De l'interdépendance entre ces phases se décline ensuite naturellement la définition des exigences de sécurité de haut-niveau (appelées ici « objectifs »), puis de bas-niveau (appelées « exigences »), conformément à **ISO 15408** et **ISO 17799**. Cette dernière phase permet de sélectionner les bonnes contremesures strictement adaptées aux besoins de l'organisation. Tous les concepts présentés dans la première partie sont donc présents, malgré des différences de terminologie. Quant au processus de gestion des risques, les phases 5 et 6 vues précédemment ne sont pas réellement développées, ce qui ne permet pas de valider véritablement le cycle théorique dans son ensemble. Dans ce cas, certains considèrent alors EBIOS exclusivement comme une méthodologie d'analyse des risques.

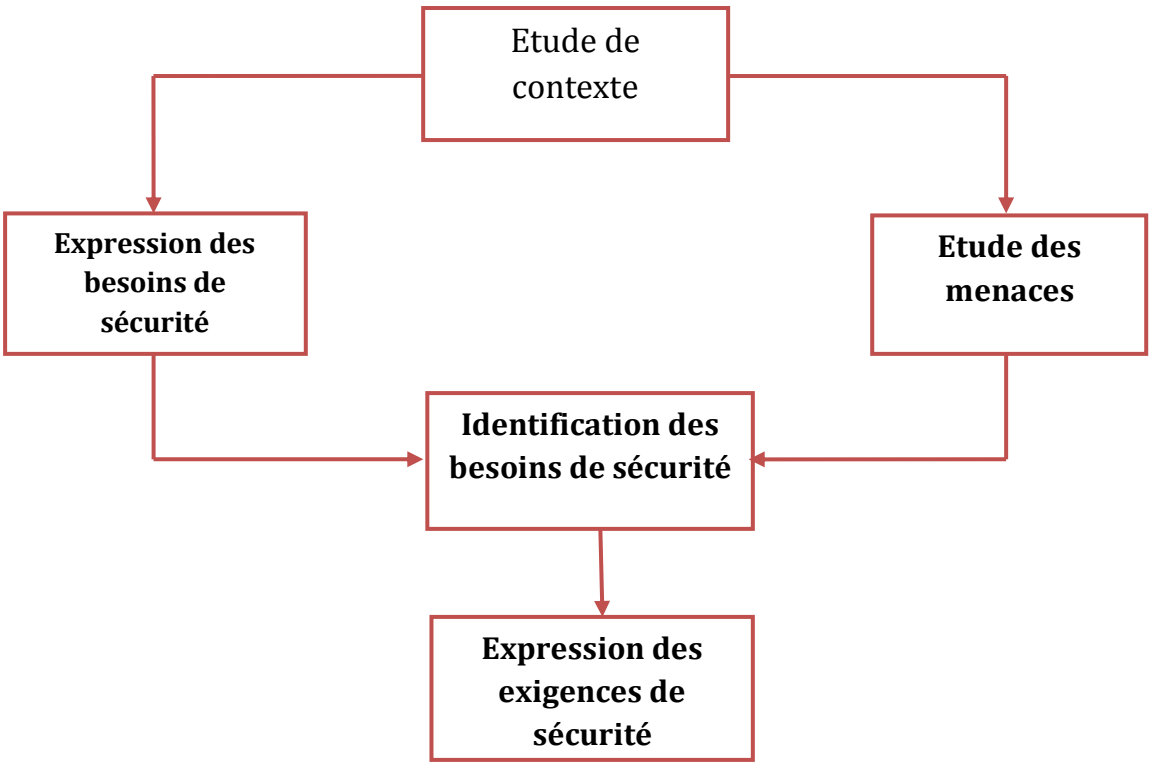


Figure 1: Schéma méthode EBIOS

2. OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)

C'est une méthode d'évaluation publiée par le SEI (Software Engineering Institute) de la Carnegie Mellon University de Pittsburgh aux États-Unis, université très reconnue dans le domaine de la sécurité. En se basant sur les travaux du CERT[11] Américain, l'équipe du SEM (Survivable Enterprise Management) a développé cette méthode d'évaluation des vulnérabilités, des menaces, et des actifs opérationnels critiques. L'ensemble de la méthode est public et maintenu par l'université. La méthode OCTAVE se compose en trois phases:

1) Vue organisationnelle,
2) Vue technique,
3) Développement de la stratégie de sécurité.

[11] Computer Emergency Response Team (US CERT)

Elle est centrée sur la protection des actifs de l'entreprise et le management du personnel. Elle couvre l'ensemble des processus métiers de l'entreprise aux niveaux organisationnel et technique. Cette méthode suppose la constitution d'une équipe pluridisciplinaire comprenant des membres de tous les services de l'entreprise. Elle leur permettra d'améliorer leur connaissance de leur entreprise et de mutualiser les bonnes pratiques de sécurité.

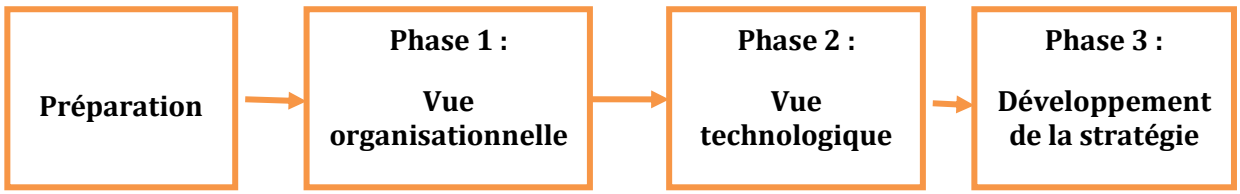


Figure 2: Schéma méthode OCTAVE

3. MEHARI (Méthode Harmonisée d'Analyse des Risques)

MEHARI est une méthode d'analyse des risques mise au point en 1996 par le Club de la sécurité de l'information français (CLUSIF). Elle s'inspire de la méthode MARION, elle aussi mise au point par le CLUSIF.

MEHARI a pour but d'aider les entreprises et organismes à sécuriser leurs systèmes d'information. Elle est très utilisée en France, en Europe et également au Québec. La démarche générale de MEHARI consiste à diagnostiquer l'état de la sécurité, l'analyse des enjeux de sécurité avec une classification préalable des entités du système d'information en fonction de trois critères de sécurité de base (confidentialité, intégrité, disponibilité). MEHARI dispose également d'une base de connaissance des services de sécurité et pourra être employée pour bâtir un référentiel de sécurité (politique de sécurité) contenant l'ensemble des règles de sécurité à respecter dans l'entreprise. MEHARI demeure une des méthodes d'analyse des risques les plus utilisées actuellement. Elle est dérivée de deux autres méthodes d'analyse des risques (MARION et MELISA).

MEHARI est maintenue en France par le CLUSIF (Club de la Sécurité des Systèmes d'Information Français), via notamment le Groupe de Travail dédié à cette méthode. Cette méthode se présente comme une véritable boîte à outils de la sécurité des SI, permettant d'appréhender le risque de différentes manières au sein d'une organisation, et composée de plusieurs modules. Ces derniers, indépendamment de la démarche sécurité choisie, permettent notamment :

- **D'analyser les enjeux de la sécurité** (en décrivant les types de dysfonctionnements redoutés) et, corrélativement, de classifier les ressources et informations selon les trois critères de sécurité de base (Confidentialité, Intégrité, Disponibilité).
- **D'auditer les services de sécurité**, de manière à prendre en compte l'efficacité de chacun, son contrôle, et de synthétiser les vulnérabilités.
- **D'analyser les situations de risques**, permettant d'évaluer les potentialités et les impacts intrinsèques, ainsi que les facteurs d'atténuation de risque, puis, enfin, de déduire un indicateur de gravité de risque. MEHARI présente une grande diversité dans l'utilisation de ses modules.

Trois approches se détachent plus particulièrement :

a) En se basant sur une analyse détaillée des risques, il est possible de mettre en œuvre des plans de sécurité. Cette démarche se décline au niveau stratégique, mais aussi opérationnel.
b) En se basant sur l'audit de sécurité, ou plus précisément après un diagnostic de l'état de sécurité, la réalisation de plans d'actions est facilitée. En effet, des faiblesses relevées découlent alors directement, les actions à entreprendre.
c) Dans le cadre de la gestion d'un projet particulier, il faut tenir compte de la sécurité, en se basant sur l'analyse des risques et ainsi faciliter l'élaboration de plans d'action. Les besoins de sécurité sont alors directement intégrés aux spécifications du projet, et à intégrer dans le plan de sécurité global de l'entité concernée. Cette méthode s'aligne avec

les deux premières en termes de couverture du processus de gestion des risques.

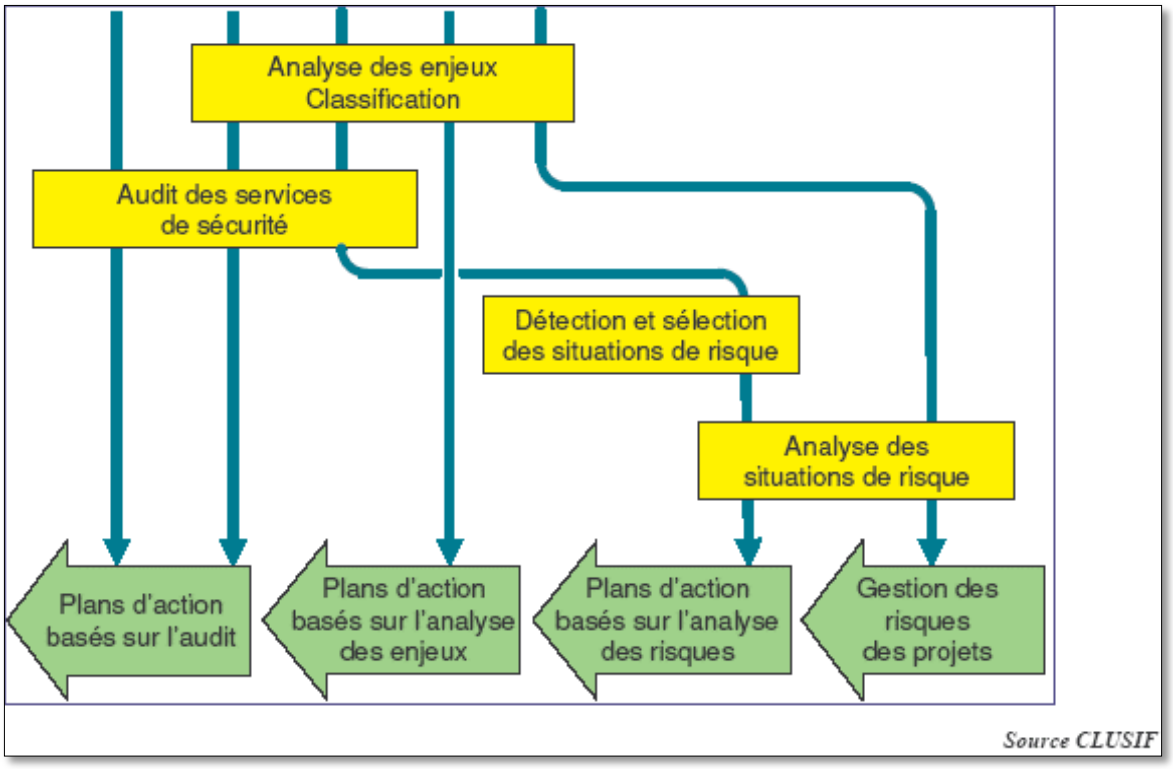


Figure 3: Schéma méthode MEHARI

4. CRAMM (CCTA Risk Analysis and Management Method)

CRAMM a été inventée par la compagnie Siemens et l'agence centrale de traitement des données et des télécommunications du gouvernement Britannique. Il s'agit d'une méthode d'analyse qualitative du risque et un outil de management développée par l'Agence centrale de l'informatique et des Télécommunications du gouvernement britannique. Conforme aux normes BS7799 et ISO 17799, CRAMM est applicable à toutes les étapes du cycle de vie du système d'information de tout organisme. CRAMM est constituée de trois étapes :

- l'établissement des objectifs de la sécurité (identification et évaluation de l'existant),

- évaluation des menaces et des vulnérabilités,
- sélection des remèdes (contremesures) et recommandations.

CRAMM est payante et propose une base de connaissance (librairie) très riche contenant plus de trois milles contre-mesures détaillées, organisées en soixante dix groupes logiques. CRAMM fournit aussi des logiciels pour la mise en œuvre de la méthode qui permettent de faire des simulations, des rapports et le suivi des mesures (contre-mesures) de sécurité. Il existe deux variantes de CRAMM, à savoir :

- CRAMM Express : qui permet de faire un état de la sécurité du SI en limitant les points de contrôle (contre-mesures) à contrôle
- CRAMM Expert : qui se positionne comme l'outil de sécurité de l'information professionnel, pour réaliser des analyses détaillées des risques, y compris ceux destinés à soutenir la conformité ISO 27001 ou les programmes de certification.

5. ITIL (Information Technology Infrastructure Library)

L'acronyme traduit en français donne une idée plus claire de ce qu'est ITIL, *Information Technology Infrastructure Library* ou bibliothèque d'infrastructure des technologies de l'information. Il s'agit d'une bibliothèque, ensemble de livres dans lesquels sont reprises et consignées de nombreuses pratiques, procédures et méthodes permettant de gérer les systèmes d'information.

Contrairement à celles précitées, ITIL n'est pas une méthode mais un grand recueil des « meilleures pratiques », mais qui utilise certaines des méthodes (EBIOS, MEHARI, etc.).

ITIL présente un côté très flexible qui permet de l'adapter très facilement à la réalité rencontrée dans une entreprise donnée. Cette caractéristique constitue l'une des raisons de son grand succès au niveau mondial. En outre, depuis janvier 2006 ITIl est couplée avec la norme ISO 20000 reposant sur la norme britannique BS 15000.

La philosophie d'ITIL repose sur quatre concepts fondamentaux :

- **Le premier** d'entre eux est la prise en compte de l'attente du client dans la mise en œuvre des services informatiques que les anglophones appellent le Customer Focus
- **Le second** principe correspond aux cycles de vie des projets informatiques qui doivent intégrer dès leur naissance les différents aspects de la gestion des services informatiques
- **Le troisième** concept fondateur préconise la mise en place des processus ITIL interdépendants permettant d'assurer la qualité des services.
- **Le quatrième** et dernier principe correspond à la mise en place d'une démarche qualité pour les services installés et d'une mesure de cette qualité effectuée du point de vue des utilisateurs

DEUXIEME PARTIE

LA SECURITE N'EST PAS SEULEMENT UN ENJEUX TECHNOLOGIQUE

Protéger les informations sensibles de l'entreprise contre des manipulations non autorisées et empêcher la divulgation par les personnes qui y ont légitimement accès, est devenu une préoccupation majeure pour toutes les entreprises grandes ou petites. Employés, dirigeants, partenaires, clients, etc., constituent une menace potentielle importante pour l'entreprise, vu leurs connaissances et leurs accès autorisés aux systèmes d'informations. De nombreuses organisations réduisent la sécurité de leurs systèmes d'informations à la mise en place de pare-feu et d'installations de solutions antivirales. Or, ces dispositifs s'avèrent être totalement inefficaces quand il s'agit par exemple d'attaques de type « *Ingénierie sociale ou Social Engineering* ». En effet dans certains cas, pour obtenir des informations aussi critiques soient-elles, il suffit juste de le demander aux personnes qui les détiennent comme cela se fait dans l'ingénierie sociale. Des attaques informatiques sophistiquées ayant comme pré-requis un bagage technique évolué et des outils technologiques de pointe, ne sont plus nécessaires. Face à ce genre de menaces, la protection physique et logique du SI, aussi robuste soit-elle, ne sert simplement à RIEN.

En outre la dimension organisationnelle de la sécurité informatique est souvent négligée à tort. Ce n'est assurément pas par manque de moyens techniques de protection, que des organisations comme la CIA, le FBI, AT&T, Microsoft ou même la NASA, Amazon, le Ministère du travail Américain, ont été victimes d'incidents informatiques. Ces organisations disposent pourtant de moyens colossaux pour assurer un niveau de sécurité très élevé de leurs SI. On en déduit alors aisément que la faille est plutôt organisationnelle, voir humaine.

Bien évidemment, investir en matière technologique est inévitable pour mettre en place les outils nécessaires à la prévention, détection et correction des failles de sécurité. Il est clair que la sécurisation de l'entreprise coûte très cher, surtout pour les grandes entreprises dont les succursales sont dispersées au sein d'un même pays ou à travers le monde. Ceci dit, l'aspect organisationnel constitue la base de toute politique sérieuse de sécurisation des Systèmes d'Informations.

Même si le périmètre à couvrir est réduit dans les TPE/PMI, ceci ne signifie pas nécessairement qu'elles sont totalement à l'abri des attaques et incidents informatiques. De plus en plus d'attaques ciblant les TPE / PME déjà fortement secouées par l'orage économique mondial, sont menées dans le but d'utiliser ses cibles faciles et moins rentables pour en atteindre de plus grosses (*drive by download, whater hole*).

L'aspect organisationnel consiste à mettre en place une politique de sécurité de l'information, une charte d'utilisation des ressources et l'ensemble des processus et procédures opérationnelles permettant d'assurer un niveau de sécurité minimal. D'ailleurs, très souvent lors des audits de sécurité, l'on constate que le volet technologique et technique est plus ou moins maîtrisé et que la nature des failles est dans la majorité des cas, organisationnelle. On estime entre 60 et 80%, la proportion du risque dû à des facteurs « internes » pour une société, ce qui signifie que la protection vis-à-vis d'attaques externes est relativement bien maitrisée.

L'absence de politique de sécurité, le manque de formalisation du mode opératoire de la sauvegarde, le manque de l'inventaire des actifs critiques, le manque de garanties juridiques de protection de l'information, sont quelques exemples de lacunes en matière de sécurité organisationnelle.

Comme indiqué plus haut, l'ingénierie sociale (social engineering en anglais) est une forme d'escroquerie utilisée en informatique pour obtenir un bien ou une information. Cette pratique exploite l'aspect humain et social de la structure à laquelle est lié le système informatique visé. Utilisant ses connaissances, son charisme, l'imposture ou le culot, le pirate abuse de la confiance, l'ignorance ou la crédulité de personnes possédant le bien informationnel qu'il tente d'obtenir (informations en l'espèce). Il serait donc intéressant de mettre un peu plus l'accent sur ce qui est considéré par les experts de la sécurité comme le maillon faible de la chaîne de sécurité, c'est-à-dire **l'HOMME.**

« La résistance d'une chaîne se mesure à la force de son maillon le plus faible »

1 L'ETRE HUMAIN : LE MAILLON FAIBLE DE LA CHAINE DE SECURITE

" *Ne vous fiez pas aux protections et aux pare-feu pour protéger vos informations. Surveillez les points les plus vulnérables. Vous constaterez que c'est votre personnel qui constitue le maillon faible* " *L'art de la Supercherie',* Kevin D. Mitnick et William L. ; éditions Campus Press.

Dans le monde de la sécurité TI, l'on croit trop souvent que les cybercriminels sont beaucoup plus ingénieux et savants que les professionnels assignés à la sécurisation des SI. Or, selon le célèbre hacker Kevin Mitnick[12], presque toutes les failles de haut niveau (critiques) sont le résultat d'une violation des processus métiers et/ou règles procédurales ou de l'ingénierie sociale, mais non le fait d'un savoir faire technique exceptionnel.

[12] Kevin Mitnick est considéré comme le plus célèbre hacker de ses dernières décennies et est le père de l'Ingénierie sociale

§1 LE CERVEAU ET LE RAISONNEMENT HUMAIN

Le comportement et le raisonnement humain sont marqués à la fois par les propriétés biologiques du cerveau et par les caractéristiques des situations dans lesquelles les personnes se trouvent placées. Beaucoup d'analogies sont faites entre le fonctionnement du cerveau humain et celui d'un ordinateur. Elles conduisent souvent à des conclusions fausses sur les raisonnements en situation de travail. Quelques propriétés du cerveau et du traitement humain de l'information méritent d'être relevées et prises en compte.

1. La perception

Les capteurs qui permettent notre perception ne sont pas passifs, c'est-à-dire exclusivement réactifs. Par exemple, les yeux ne sont pas comme une caméra qui se contenterait de transmettre des images qui se trouvent dans son champ visuel et selon une configuration bien déterminée. Les yeux explorent l'espace, guidés par le cerveau. L'information est recherchée activement, en fonction de l'action qui est en cours et de l'expérience de la personne. C'est-à-dire que des informations qui ne sont pas recherchées seront perçues beaucoup moins facilement que celles qui le sont.

La recherche active d'informations favorise la perception de tous les sens. En effet, le cerveau les prépare à détecter certaines informations. Celles qui ne sont pas recherchées devront avoir des caractéristiques physiques beaucoup plus fortes pour être perçues. La perception est ainsi à la fois descendante (guidage par le cerveau) et ascendante (les informations recueillies vont modifier la suite de l'exploration).

Focalisation de l'attention quand on attend le bus : les véhicules qui passent et qui ne sont pas des bus seront à peine perçus. Si un bus arrive, la perception va se modifier pour se focaliser sur le numéro et non plus sur la forme générale du bus.

Le cerveau concentre son attention sur ce que nous définissons comme prioritaire, à un instant donné.

2. La reconnaissance des formes

Les informations disponibles à nos sens sont infiniment nombreuses. Leur traitement n'est pas effectué de façon analytique : c'est-à-dire que notre cerveau distingue directement des formes, des configurations, dont certaines sont innées (distinguer la forme d'un visage humain) et d'autres acquises. Le cerveau sélectionne et combine des figures de façon à les rapprocher d'une unité cohérente connue. Cette capacité à identifier des configurations globales permet à l'être humain de « reconnaître » rapidement une configuration qui « ressemble » à une autre, sans pour autant être exactement semblable. C'est en général un avantage, puisque cela permet de traiter des situations par analogie. Mais c'est parfois un inconvénient, si ce qui était important ce jour-là était la différence et non la similarité.

3. Un traitement variable

Le cerveau est « une glande », c'est-à-dire une structure anatomique qui a pour fonction la production et la sécrétion de substances hormones (enzymes digestives, sueur, salive, lait, etc.). Le système nerveux n'est pas semblable à un câblage électrique, même s'il est vrai que dans les neurones, l'influx nerveux (électrique) se propage de façon stable, sauf maladie neurologique. Mais chaque neurone est en relation avec plusieurs autres en amont, et en général un grand nombre en aval. Le transport des messages nerveux entre deux neurones peut être affecté par les émotions se trouvant dans la « *fente synaptique* ». Or, l'espace synaptique baigne dans le liquide extracellulaire, qui peut contenir d'autres neurotransmetteurs,

notamment si la personne se trouve en situation d'émotions fortes, de stress, ou des dérivés de médicaments ou de drogues. La transmission synaptique donc de l'influx nerveux sera alors modifiée, les différents neurones en aval ne seront pas activés de la même façon. En effet, sous l'effet des hormones (messagers chimiques destinés à divers organes), les synapses sont sensibles aux différentes régulations de l'organisme et aux émotions. De ce fait, le traitement de l'information par le cerveau humain (sa rapidité, mais aussi parfois ses résultats) sont susceptibles d'être affectées par ces modifications endocrines.

En résumé, la transmission chimique du message (influx nerveux) est modifiée par l'état de la personne. Aussi, certaines drogues peuvent-elles augmenter ou diminuer la vigilance, le champ visuel, la vitesse de réaction, la perception de la douleur, la mémoire à court terme, etc. L'état psychique de la personne va alors modifier les « drogues internes » de l'organisme, avec des effets tout à fait comparables.

4. La mémoire

La mémoire relève de trois processus différents :

- ***La mémoire sensorielle*** : C'est une sorte de « mémoire-tampon » où les informations issues de la perception sont stockées moins d'une seconde avant d'être traitées. Après ce délai, si elles n'ont pas été traitées, elles sont perdues.
- ***La mémoire à court terme*** : C'est le résultat d'une première sélection (qui dépend du modèle mental de la personne et de l'orientation de l'action à ce moment), et donc d'un filtrage. C'est l'information sur la situation présente, disponible pour traiter celle-ci. Elle comporte les caractéristiques suivantes:

– d'une capacité très limitée en nombre d'unités d'information qu'elle peut retenir ;
– très sensible aux interférences ;

– la mémoire des informations de nature langagière peut être entretenue par autorépétition, mais il n'en est pas de même de la mémoire précise d'une couleur ou d'une sensation.

  La mémoire à court terme est de ce point de vue, un point faible du fonctionnement humain, et il est dangereux de faire reposer la sécurité sur cette fonction.

- ***La mémoire à long terme*** : Elle contient les traces des situations que nous avons vécues. Elle est d'une capacité virtuellement illimitée, mais possède une propriété très particulière : *il est impossible de savoir si quelque chose est en mémoire*. La possibilité d'accéder à une information en mémoire à long terme dépend notamment de la ressemblance entre les circonstances d'acquisition et les circonstances de rappel. La mémoire à long terme peut être n'est pas simplement un stock de souvenirs. Pour un opérateur ayant peu d'expérience, la réponse à une situation inhabituelle passera souvent par l'application d'une règle formelle apprise ou recherchée dans un manuel. Chez les opérateurs expérimentés, il s'est développé des schèmes d'action, des unités mentales qui mettent en relation les éléments perçus et les actions à effectuer. Ce fonctionnement est beaucoup plus économe en ressources que le premier.

5. Un apprentissage permanent

L'être humain apprend ainsi en permanence, stockant et synthétisant les traces de son expérience. Il apprend aussi, bien sûr, dans des moments conçus comme des périodes de formation. Mais il n'est pas certain que les connaissances qu'il acquiert en formation constituent un tout harmonieux avec celles qui résultent de l'expérience. Si, en situation de formation, sont recréées des situations voisines de celles qui sont vécues dans le cadre professionnel, les nouvelles connaissances pourront être intégrées à la synthèse réalisée par le cerveau sur ces familles de situations. Sinon, il est probable qu'elles seront classées avec beaucoup d'autres

énoncés, prêts à ressortir uniquement dans une situation ressemblant à une situation scolaire.

6. Le cerveau tourné vers le futur et ses simulations

Le cerveau, nous l'avons dit, ne se contente pas d'attendre que les informations lui parviennent. À partir de son anticipation des conséquences de l'action en cours, il commande l'exploration perceptive, prédit les informations qu'elle devrait rapporter et contrôle par échantillonnage que les choses se passent comme prévu. Le cerveau réalise en permanence des prédictions, en utilisant les souvenirs de configurations similaires. Il simule les conséquences de différentes actions possibles, en activant les mêmes voies nerveuses que si l'action était vraiment effectuée. Dans ce cas de figure, seule la réalisation est inhibée.

En outre, le cerveau compare ainsi différentes possibilités d'action et leurs conséquences en projetant sur le monde réel ce qu'il a synthétisé par expérience. Cette propriété rend l'être humain très performant pour traiter des situations similaires à celles qu'il a déjà vécues, mais un peu différentes.

§2 *DES OPERATEURS HUMAINS DIFFERENTS ET VARIABLES*

L'être humain a des propriétés résultant de son fonctionnement biologique, et qui ne peuvent être modifiées à volonté. Elles doivent être prises en compte dans la conception des systèmes de travail, au même titre que les propriétés physicochimiques des matériaux. Si ce n'est pas le cas, l'être humain s'adaptera plus ou mois bien dans certaines limites, mais toujours à un coût élevé pour lui et avec une dégradation de sa performance. Nous ne nous hasarderons pas à tenter de présenter ici, l'ensemble des propriétés du fonctionnement humain qui peuvent

entrer en jeu dans le travail, vu l'extrême complexité du sujet. Ce chapitre présentera brièvement, d'abord quelques éléments de la diversité des individus, puis les variations de l'état du corps en fonction des moments de la journée, qui doivent être prises en compte dans la conception de la sécurité informatique.

1. La santé physique et l'âge

Avec l'âge, les principales restrictions médicales d'aptitude concernent le travail de nuit, les efforts notamment à la chaleur, et les sollicitations du dos, de la mémoire et de l'acuité visuelle. Elles sont susceptibles de mettre en difficulté à la fois les personnes concernées et l'entreprise, pour laquelle la gestion des ressources humaines devient plus complexe.

2. La fatigue

La fatigue implique une baisse de la capacité de l'organisme et nécessite donc la mise en œuvre de mécanismes physiologiques différents, à un coût plus élevé, quand le même niveau d'activité doit être maintenu. En effet, être fatigué, c'est devoir mobiliser plus de ressources pour arriver au même résultat. On distingue la fatigue musculaire et la fatigue nerveuse.

La fatigue musculaire traduit l'épuisement des ressources énergétiques internes au muscle, une augmentation de son acidité, et le fait que la circulation sanguine est insuffisante pour évacuer les déchets et apporter le glucose et l'oxygène nécessaires.

La fatigue nerveuse quand à elle, traduit l'impossibilité pour le système nerveux de maintenir le traitement de l'information au même rythme. Elle débouche sur une augmentation des erreurs et des omissions, et une dégradation de la perception. Elle peut aussi donner lieu à des signes d'irritabilité. Dans un premier temps, la fatigue

n'est pas consciente, les capacités sont affectées, mais la personne ne s'en rend pas compte. Dans un deuxième temps, celle-ci perçoit la fatigue et pourra éventuellement mettre en place des stratégies pour la gérer (demander de l'aide, multiplier les vérifications). Du point de vue de la sécurité, la phase inconsciente de la fatigue est particulièrement critique.

La fatigue nerveuse apparait comme un facteur très important à prendre en compte dans la mise en œuvre de la sécurité informatique, du fait qu'elle est susceptible d'avoir une incidence directe sur la gestion du SI.

3. Les événements de la vie

Les événements de la vie (conflit, deuil, échec. . .) et les émotions qui en résultent peuvent affecter l'état physique de la personne, sa perception, ses prises de décision. Par exemple, la recherche d'informations sera plus limitée, les raisonnements intégreront moins de facteurs, les décisions seront moins nuancées. Si ces événements sont d'origine individuelle (familiale), les autres membres du collectif de travail pourront en général compenser les variations de l'état de la personne concernée. Si en revanche l'origine est collective (conflit avec la hiérarchie, incident occasionné par un maillon de la chaîne de sécurité), il s'agit d'un « mode commun », et c'est toute la capacité perceptive et décisionnelle de l'équipe qui peut se trouver modifiée.

4. Les rythmes biologiques

L'organisme humain, comme celui d'animaux et de végétaux, comporte des horloges internes. Différents phénomènes biologiques sont périodiques, la plupart avec une période de l'ordre de 24 heures (il existe aussi des rythmes mensuels, annuels). La température, la sécrétion de nombreuses hormones, la vigilance, la

performance sensorimotrice, etc., varient ainsi au cours d'une journée. La perturbation des rythmes biologiques, due aux décalages engendrés pendant le service a des effets néfastes sur la santé, la vigilance, la productivité, etc. Il est totalement illusoire d'espérer que la vigilance et la rapidité de réaction à 3 heures du matin soient les mêmes qu'à 15 heures, cela est physiologiquement impossible.

§3 LES SITUATIONS DE TRAVAIL

1. Le stress au travail

Le stress est d'abord une réponse de l'organisme à une situation susceptible de menacer son intégrité. Des ressources biologiques exceptionnelles sont alors mobilisées pour pouvoir faire face à cette menace.

Le stress au travail peut être définit comme étant « un état accompagné de plaintes ou dysfonctionnements physiques, psychologiques ou sociaux, et qui résulte du fait que les travailleurs se sentent inaptes à combler un écart entre leurs possibilités et les exigences ou les attentes les concernant ». Le stress n'est pas une maladie mais une exposition prolongée au stress peut réduire l'efficacité au travail et causer des problèmes de santé. La réponse biologique se fait en deux ou trois temps :

- ***Premier temps*** : L'alerte

Le système nerveux agit sur la partie centrale des glandes surrénales, qui secrètent des catécholamines (adrénaline, noradrénaline). Celles-ci vont provoquer la mobilisation de stress. Alors la pression artérielle augmente, le sang est dirigé de préférence vers les muscles et le cerveau, le sucre disponible dans le foie est mis en circulation dans le sang. Cette réaction rapide conduit à une mobilisation d'énergie à court terme qui permet de faire face à la situation immédiate, mais qui épuise les

sources énergétiques habituelles. On peut aussi noter qu'à faible dose, la noradrénaline favorise un raisonnement élaboré, tandis qu'à dose élevée, elle conduit le cerveau à privilégier les programmes de réponse stéréotypée les plus anciennement appris, et la préservation immédiate plutôt que le moyen terme.

- ***Second temps*** : la résistance

Si la source de stress persiste, l'organisme doit chercher d'autres ressources. L'hypothalamus puis l'hypophyse envoient des messages chimiques qui commandent à la partie périphérique des glandes surrénales la sécrétion de cortisol. Celui-ci permet la production de sucres à partir des graisses et des protéines. Il a également des effets anti-inflammatoires, mais le maintien d'un taux élevé de cortisol a des effets toxiques pour l'organisme : il entraîne la récupération a des perturbations métaboliques, génératrices à terme d'athérosclérose (obstruction des artères) et de maladies cardiovasculaires, et une diminution des défenses immunitaires.

- ***Troisième temps*** : l'épuisement

Si la source de stress devient chronique, il arrive un moment où l'organisme renonce à réagir. Les régulations biologiques (notamment celle qui ajuste la production de cortisol) sont un stress permanent débordées, et de nombreuses pathologies peuvent apparaître (atteintes cardiovasculaires, maladies infectieuses, allergiques, cancers). Une issue possible chez l'être humain est la dépression. Celle-ci se traduit notamment par une perception négative indifférenciée des situations, et une « surgénéralisation », c'est-à-dire une tendance excessive à attribuer des traits communs à des situations différentes, qui empêche de traiter de façon nuancée des contextes distincts. Un tel état de forme d'un employé chargé de la sécurité du système d'information à un niveau élevé, peut être très dommageable pour l'entreprise et le risque ultime est le suicide.

2. Les conditions sociales et l'environnement social

La nature et les causes criminogènes de la fraude informatique sont très complexes. En effet, beaucoup de chercheurs considèrent que l'employé commettant une fraude informatique est motivé avant tout par l'avidité, l'égoïsme et l'individualisme qui sont inhérents aux valeurs de la société capitaliste. Tout cela, associé aux émotions et besoins humains, en fait la première motivation de criminalité informatique. Il n'est cependant pas facile de lier la criminalité informatique à des pathologies individuelles et en conséquence, quasiment impossible d'établir un portrait type. Mais il ne faut pas tomber dans l'excès contraire en considérant que les faits de criminalité informatique ne sont dus qu'à des cas isolés. Il est donc nécessaire d'analyser les relations **individu - organisation - facteurs sociologiques**. Ceci implique une bonne connaissance des pratiques de l'entreprise elle-même, ainsi que les valeurs culturelles qui généralement favorisent ou pas la fraude, car la culture (le vécu) est prédominante chez l'homme.

Le manque de mesures de sécurité crée un environnement dans lequel les employés ne se sentent en aucune façon responsable des conséquences de leurs actions. Une telle situation contribue certainement à la fraude, car le facteur situationnel lié à un environnement propice à la genèse d'idées criminelles, est très important. Le facteur situationnel joue un rôle déterminant dans le passage à l'acte criminel, notamment la fraude informatique. En effet, l'absence de tout contrôle et l'accès facile aux données sensibles de l'entreprise, peut être un élément déclencheur de réactions criminelles. Cela démontre que les dirigeants ont une responsabilité énorme dans la sécurité de leur entreprise, puisque de par leurs décisions, ils influencent directement la structure de cette entreprise et donc l'occurrence de la fraude.

A l'heure qu'il est, les études empiriques officielles relatives à la fraude informatique en interne (dans les entreprises), sont jusque là inexistantes en Côte d'Ivoire. Cet état de fait traduit que la compréhension de la fraude informatique et

la sécurité informatique n'ont pas encore acquis la place qu'elles méritent dans l'environnement économique Ivoirien.

2 LA CULTURE MANAGERIALE EN ENTREPRISE

Selon les experts en gestion des ressources humaines, la *gestion des choses* ou gestion du personnel (management comptable, technique, administratif) remplace progressivement le « *gouvernement des hommes* » (management des équipes, et des processus humains). Or, l'homme représente le capital de compétences, de professionnalisme, d'engagement, d'innovation, d'initiatives et de performance qui garantit la réussite et la pérennité des entreprises, petites et grandes. La question qui se pose est de savoir si la Direction des Ressources Humaines, n'est vouée exclusivement qu'à la *gestion des choses* ou gestion du personnel ; ou doit-elle s'ouvrir un peu plus au *gouvernement des hommes* (management des équipes). On voit naitre, au delà de toutes considérations idéologiques, le besoin de construire ou reconstituer une culture managériale qui puisse associer:

- la compétence humaine des managers,
- la compréhension des phénomènes collectifs et des pratiques de management des hommes
- le développement d'une culture spécifique qui intègre l'originalité singulière et la diversité de chaque entreprise.

En somme, il est question de « repositionner l'homme au cœur du système », en créant les conditions d'un alignement individuel fort avec les valeurs de l'entreprise. « *Car si l'on veut sortir du domaine de l'incantatoire en matière de sécurité, il faut que les "aveugles" que sont les managers et les directions, retrouvent la vue et que les "muets" que sont les collaborateurs puissent s'exprimer* ».

La simple communication d'une charte de valeurs est insuffisante, quoique claire ou contraignante. Il est nécessaire d'établir un substrat managérial fort en matière de conception de la sécurité.

§1 LA CULTURE DE SECURITE

Le terme "culture" désigne tout d'abord un ensemble de valeurs, de représentations et de pratiques partagées par une communauté. La sécurité quand à elle traduit l'absence de risque majeurs ou du moins jugé acceptables. En un mot, la culture de sécurité désigne l'ensemble des caractéristiques et des attitudes, qui dans les organismes (entreprises, associations, administrations) et chez les individus font que les questions relatives à la sécurité, bénéficient en priorité de l'attention qu'elles méritent en fonction de leur importance.

Parler de la culture de sécurité en entreprise indique donc clairement la volonté de relier deux sphères qui sont : d'une part, ***celle des comportements et des valeurs des acteurs*** (tant internes, qu'externes à l'entreprise) et d'autres part, ***celle de l'organisation et des structures des secteurs à risques***. Cette distinction permet de relever les deux grands champs d'application de la sécurité que sont : l'entreprise et la société civile, qu'il est important de rapprocher et sur lesquels il s'impose d'agir dans le but de faire de la sécurité une culture partagée. Enjeux majeure pour l'entreprise, la sécurité informatique nécessite donc d'orienter la démarche sur un développement de la culture de sécurité de l'entreprise et de ses composantes. Au sein de l'entreprise, cela passe avant tout par l'action sur deux axes internes à l'entreprise qui sont :

- Engagement de la direction
- Système de management de la sécurité

1. Engagement de la direction

L'engagement de la direction est le socle de la culture de sécurité en entreprise. Il favorise la diffusion de la culture de sécurité dans les différents niveaux de l'entreprise. Cet engagement pour être efficient doit aller au delà du le simple effet d'affichage, et s'étendre à l'élaboration d'une politique claire, participative et relayée par des actes visibles à tous les niveaux de l'entreprise. En effet, la culture de sécurité se transmet de façon descendante, c'est-à-dire qu'elle part des instances dirigeantes au sommet de l'organigramme hiérarchique (leaders), jusqu'aux simples employés, à la base de l'organigramme de l'entreprise, acteurs majeurs de la vie de l'entreprise.

2. Système de management de la sécurité

Le système de management de la sécurité quant à lui intègre différents axes, qui sont:

- ***La mise en œuvre d'une politique organisationnelle*** (structures règles, hiérarchies) :

Il s'agit de mettre sur pieds des structures intégrant l'objectif de développement de la culture de sécurité :

- en définissant clairement les responsabilités de sortes à impliquer chacun des acteurs,
- en élaborant des procédures visant au développement de la culture de sécurité,
- en définissant des modalités de contrôle de l'efficacité des mesures adoptées et de suivi des indicateurs.

- ***L'intégration de la culture de sécurité dans les comportements des acteurs de l'entreprise***

La sécurité ne saurait s'atteindre uniquement à travers une démarche directive de type Top down (directives unilatérales venant de la haut, à exécuter). Il est important de susciter l'adhésion des acteurs à la démarche, à travers une approche similaire que celle utilisée par les spécialistes de la publicité, dite de « connivence ». Développer une culture de sécurité, c'est favoriser l'implication de tous les acteurs à l'adoption de comportements participatifs. Ceci implique une responsabilisation, vis-à-vis de la prévention, de la protection, de l'analyse des risques, et une reconnaissance de l'importance du rôle joué par chacun des acteurs quelque soit le niveau de responsabilités.

- ***La mise en place de lien fonctionnels entre l'organisationnel et les comportements***

Développer une culture de la sécurité revient à construire une cohérence entre les règles et les comportements, entre le discours et la pratique, pour faire de la sécurité une valeur partagée par tous, au sein de l'entreprise. La véritable difficulté reste l'application et la mise en œuvre effective de la fonctionnalité de liens entre l'organisation et les comportements. Pour ce faire, certains principes sont à prendre en compte. Ce sont ces principes que nous étudierons dans les points suivants.

§2 LA GESTION DES RESSOURCES HUMAINES

La gestion des ressources humaines (GRH) peut être définie sommairement, comme la gestion des hommes au travail dans des organisations. La gestion des ressources humaines est une discipline complète qui va au delà de la simple administration du personnel, comme c'était le cas avant les années 1980. Cet élément capital pour la vie et la croissance des entreprises, comporte plusieurs facettes, à savoir : gestion

des recrutements et des affectations, des carrières, de la rémunération, du dialogue social, de l'hygiène de sécurité, etc. Cette liste non-exhaustive des différentes composantes de la gestion des ressources humaines montre l'importance de cet outil dans le management de l'entreprise. Elle est dans le prolongement des règles organisationnelles à prendre en compte dans l'établissement de la culture de sécurité.

1. Le rôle du management dans l'entreprise

Le rôle du management des ressources humaines au sens strict, c'est de concilier au mieux les intérêts de l'entreprise avec ceux des employés. Il s'agit entre autres de mettre en œuvre des actions permettant d'atteindre les objectifs fixés par la direction. En d'autres termes, la gestion des ressources humaines ramène à :

- Faire s'approprier et partager les objectifs fixés par la direction,
- Réussir à convaincre et motiver les équipes,
- Partager les informations et les connaissances,
- Créer de la cohésion (encourager et développer l'esprit d'équipe),
- Recadrer les actions,
- savoir déléguer tout en exigeant un rendu-compte régulier,
- développer les potentialités au sein des équipes,
- recadrer s'il y a débordement et résoudre les conflits etc.

L'analyse de tous ce qui suit conduit à considérer la sécurité en entreprise selon une « approche marketing ». En effet, la sécurité en entreprise dans tous les domaines, tend à devenir un « produit/service » à développer, à promouvoir à l'intérieur et à l'extérieur de l'entreprise, étant donné que les grands principes du marketing s'y appliquent. La culture de la sécurité ne peut être imposée, mais plutôt promue avec une approche de « connivence ». Les moyens mis en œuvre pour asseoir et développer une vraie culture de la sécurité en entreprise doivent s'appuyer sur la

communication (campagne de communication-marketing, organisation, formation-métier, filière management, sensibilisation, etc.).

2. La formation continue et la sensibilisation

Un accent particulier doit être mis sur la formation continue des salariés, mais aussi sur la politique de recrutement des nouveaux employés. En effet, les TIC et par ricochet la criminalité informatique sont très évolutifs, d'où la nécessité d'effectuer des mises à niveau permanentes, afin de rester au parfum des innovations technologiques et évolutions des pratiques de l'activité cybercriminelle. Une politique de formation pour les employés admis à des postes de responsabilités critiques pour la sécurité des systèmes d'information, doit être mise en place. Il ne s'agit pas juste de donner des armes technologiques aux agents, mais d'en garantir une maîtrise totale, afin de maximiser l'efficacité des employés.

L'impact d'une sensibilisation en entreprise se mesurera à l'évolution de la culture concernée ainsi qu'à certains changements de comportement attendus. « ***La sensibilisation a pour finalité de changer les regards, les mentalités et, finalement, les comportements des individus concernant des enjeux distincts liés à l'actualité de chaque organisation : promotion du développement durable, projet de changement (déménagement, nouvelle organisation, etc.), meilleure insertion des personnes handicapées dans l'entreprise, promotion de la parité, sécurité de l'information, bien-être au travail etc.*** ».

De plus, les entreprises doivent accorder un regard particulier à la diversification des domaines de spécialisation des acteurs engagés dans la sécurité de l'information. En ce qui concerne la sécurité informatique, la complexité relative de la cybercriminalité, oblige les dirigeants à accorder autant d'importance aux juristes, personnel administratif, qu'aux ingénieurs et techniciens informaticiens.

3. L'organisation du retour d'expérience

Proche dans ses principes de « l'analyse des pratiques », bien connue des professionnels du secteur social et médico-social, le «retour d'expérience » est avant tout un moment d'arrêt et de réflexion en cours d'action, destiné à identifier ce qu'il est nécessaire d'améliorer du fonctionnement d'un établissement, d'une entreprise, d'une organisation eu égard aux objectifs poursuivis. Le retour d'expérience est composé de deux phases principales : une phase de bilan de l'action réalisée et une phase de remédiation, consacrée à la recherche et à la mise en place de solutions destinées à améliorer l'action à venir. C'est ce bilan qui, conduisant à la définition de mesures correctives, constitue par la même occasion le processus d'apprentissage.

Le retour d'expérience ou **REX**, est un élément de progrès indispensable à toute organisation. Sa mise en œuvre doit être systématique après un exercice ou un événement. Au-delà de sa capacité à faire évoluer les organisations, il constitue avant tout une opportunité de partage et d'apprentissage pour l'ensemble des acteurs quels que soient leur niveau hiérarchique et leurs statuts. Il s'agit de l'analyse méthodique et rigoureuse d'un événement, ou d'un exercice dans le but de comprendre les causes et les mécanismes ayant conduit, lors de la gestion, à des innovations ou des dysfonctionnements, afin d'en tirer des enseignements pour l'avenir. Le retour d'expérience est utile pour comprendre la nature et l'amplitude des écarts entre le cadre méthodologique (contenu du PCS) et les pratiques mises en œuvre lors de la gestion de l'événement. Il conduit ainsi à faire évoluer les modes d'organisation dans le but de les rendre plus efficients. Le retour d'expérience constitue ainsi un véritable outil d'apprentissage dont l'objectif n'est pas de sanctionner mais d'apprendre toujours plus pour progresser.

Appliqué au domaine qui nous intéresse ici, le retour d'expérience permet de maîtriser par l'expérience, les enseignements tirés par la mise en œuvre de la politique de sécurité mise en place par l'entreprise, en vue de la corriger,

l'améliorer, l'adapter aux objectifs visés, en partageant les connaissances et aptitudes qui y ont découlés à toutes les échelles de la pyramide hiérarchique.

§3 POLITIQUES ET PROCEDURES

La politique de sécurité dans le domaine informatique n'est pas destinée à être un recueil de bonnes pratiques sans application. Il ne s'agit pas de définir des règles, des lois, sans en assurer une applicabilité effective (Procédure organisationnelles, chartes, référentiel, etc.).

La PSSI (Politique de Sécurité du Système d'Information) relève de nos jours, d'une vision stratégique de l'organisme et traduit un engagement fort de la direction générale. Elle s'inscrit nécessairement sur le long terme et est conforme aux dispositions législatives et réglementaires du domaine d'activité et est cohérente avec les politiques et directives de niveau supérieur (Direction Général, Ministère de tutelle, etc.). Elle se doit également d'être cohérente avec les politiques de sécurité des organismes partenaires de l'entreprise, au risque d'être un frein à son bon activité.

En plus des chartes d'utilisation, manuels et autres éléments organisationnels constitutifs de la PSSI, l'entreprise doit mettre en œuvre un plan de continuité des services (PCA, PRA) qui se doit d'être opérationnel en cas de sinistre majeur. Elle doit aussi prévoir des polices d'assurance, budgets, etc., en complément.

1. Budgets et dépenses

La sécurité du système d'information dispose-t-elle d'un budget spécifique dans les entreprises ? Quelle est la place de la sécurité des SI dans les priorités stratégiques des entreprises ?

Certaines entreprises à l'activité hautement sensible ont définit des budgets spécifiques à la Sécurité des Systèmes d'Information. Selon le JDN (Journal du Net), la part des dépenses consacrées à la sécurité des systèmes d'information dans le budget informatique global des entreprises a bondi entre 2007 et 2010. Selon le cabinet d'études Forrester Research, alors qu'elles ne représentaient que 8,2% des dépenses IT (information technologies) globales en 2007, trois ans plus tard elles pèsent désormais 14%. Pour cette année 2013, la tendance est plutôt à la hausse, voire le maintient de la part de dépense allouées à la sécurité pour les entreprises Européennes, selon le Cabinet d'Expert Pierre Audoin Consultants.

Les domaines de sécurité qui font le plein sont ceux liés à la sécurité des données et des investissements en gestion des vulnérabilités. En revanche, les entreprises ont réduit leurs dépenses en matière de gestion des accès et des identités, gouvernance et sécurisation des applications. La dernière étude de Forrester, qui a interrogé pour l'occasion 2 058 décideurs informatiques en Amérique du Nord et en Europe, met également en avant le fait que 54% des entreprises disposent d'un responsable de la sécurité des systèmes d'information rapportant directement à un membre de la direction générale.

Les études de ce genre sont bien malheureusement rares, voir inexistantes, dans les pays Africains en général. Il serait hasardeux de donner des éléments d'informations sur le sujet, tant les sources d'informations sont rares en Côte d'Ivoire. Des projets d'études sur le terrain sont formulés, mais une implication plus grande des politiques est nécessaire, afin de proposer des éléments de compréhension et de réponses au problème de la sécurité et de la criminalité informatique en entreprise.

Toutefois, il est à noter que les dépenses sont en général reparties entre logiciels et infrastructures. En effet, les dépenses de sécurité sont principalement perçues comme une couverture du risque et dans une moindre mesure, comme un gage de qualité ou un avantage concurrentiel. Elles sont plus rarement perçues comme une contrainte ou un mal nécessaire, ce sentiment étant le fait d'une mauvaise évaluation des enjeux de la sécurité informatique et une absence ou une sous-

évaluation de la fonction de RSSI (Responsable de la Sécurité des Systèmes d'Information) ou DSI (Directeur de la Sécurité Informatique), paradoxalement absent des directions générales ou des départements d'audit. La question de la création d'un département spécifique, autonome mais rattaché aux directions générales, nous paraît être un sujet très intéressant, qui mérite un intérêt particulier.

2. Externalisation

L'externalisation consiste à remettre à un prestataire extérieur une partie ou l'intégralité d'une activité qui était jusqu'alors réalisée en interne. Très souvent, l'externalisation consiste à déléguer des fonctions non stratégiques et non essentielles d'une entreprise. C'est un outil de gestion stratégique afin de restructurer l'entreprise dans sa sphère d'activités. Le développement en offshore consiste à aller chercher de la « main d'œuvre étrangère », qui serait moins chère, et donc très avantageuse au niveau financier. Cette pratique présente des avantages et des inconvénients qu'il convient de souligner. Tout d'abord, l'entreprise se détache de nombreuses contraintes qui pèsent sur son activité majeure, elle sera donc gagnante sur le plan financier. Aussi, l'entreprise qui externalise, gagne-t-elle également au niveau efficacité, puisqu'elle confit l'activité à des experts. Au vue de tous ces avantages, les entreprises ont commencé réellement à pratiquer cette stratégie au début des années 90. Depuis, le nombre de ces entreprises qui externalise tout ou partie de leur activité est croissant.

Par ailleurs, l'externalisation comporte tout de même des risques. Le premier risque non négligeable découlant d'une externalisation, est celui de la perte de confidentialité des informations. De plus, les employés ont une perte de connaissance de leur capital immatériel. L'externalisation doit être murement réfléchie, et le choix du prestataire externe est primordial. La qualité de ce dernier est indispensable pour que la stratégie s'opère de façon optimale. Ces risques doivent donc être examinés de très près par l'entreprise souhaitant externaliser une

partie ou l'intégralité de la sécurisation de son SI, sinon la stratégie peut être contre-productive.

En Côte d'Ivoire, l'externalisation de la fonction de sécurisation des SI semble acquérir un intérêt particulier. En effet, avec la politique nationale de cybersécurité mise en place par l'Etat Ivoirien, un CERT (Computer Emergency Response Team) a été mis sur pieds. Cette équipe représente à l'heure qu'il est, l'un des seuls organes sous-régionaux dotés des compétences techniques et matérielles de haut niveau nécessaires en sécurité Informatique. Composé d'Ingénieurs certifiés CEH, GSEC, GCIH, etc., issus d'établissements prestigieux de certification (EC-Council, SANS), le CI-CERT présente des garanties techniques et opérationnelles importantes. Le nouveau cadre juridique en cours d'implémentation prévoit de « *confier gestion de la sécurité* » des systèmes d'informations des entreprises et infrastructures critiques à cette équipe, dépendant de l'autorité de régulation des télécommunications.

Toutefois, vu le caractère vital que revêt le système d'Information pour les entreprises, l'externalisation partielle, c'est-à-dire, confier une certaine partie des activités de sécurisation des SI, serait un partenariat gagnant pour les entreprises Ivoiriennes.

3. Pilotage et Contrôle

Il est aujourd'hui impossible pour un DSI (directeur de la sécurité informatique) de mener à bien ses activités sans maitriser le niveau de confiance qu'il accorde à son SI. Il est devenu le comptable de la sécurité de la majorité des informations et des outils de l'entreprise. A cet effet, il doit pouvoir à tout moment rassurer sur ce point, et bien souvent indiquer quelles stratégies il compte mettre en œuvre pour accroître ce niveau de sécurité.

La sécurité du SI est désormais vitale pour l'entreprise. Tout d'abord en tant que support des processus métiers, le SI embarque naturellement de nombreux dispositifs de contrôle essentiels à la fiabilité des informations. De plus, dans de nombreux domaines (comme le contrôle des comptes), l'audit intègre de nos jours en plus des vérifications ponctuelles, une évaluation du dispositif de contrôle interne lui-même. Concrètement, le contrôle interne prends en compte ainsi toutes les mesures prises au quotidien pour maîtriser le processus (politiques, procédures, etc.) lui-même, les vérifications effectuées par les opérationnels dans le cadre de leurs activités courantes, et plus généralement la « culture de contrôle » de l'organisation. De nombreuses organisations ont ainsi défini et mis en œuvre, souvent sous la houlette du RSSI, des procédures, des responsabilités, et le reporting associé, via des démarches s'appuyant sur les méthodes ITIL, CMMI ou ISO 27001.

Comment définir sa cible en matière de contrôle permanent de la sécurité ?

Le contrôle permanent de la sécurité, qui s'inscrit dans la démarche globale de contrôle interne, se décline selon un modèle de contrôle à deux ou trois niveaux en fonction du contexte de l'entreprise.

- **Niveau 1** : Il comprend les contrôles réalisés chaque jour par les équipes opérationnelles (remontées d'indicateurs, contrôles techniques et méthodologiques, etc.). Il est intégré à leurs procédures et processus réguliers, selon le principe de « l'autocontrôle ». Il s'agit par exemple de s'assurer que les infections virales sont maîtrisées par consultation quotidienne des logs et reporting au niveau d'une console centrale, de revoir de manière régulière les droits utilisateur d'une application, de s'assurer que l'application des correctifs de sécurité se fait en accord avec la politique de sécurité, etc. Ces contrôles de niveau 1 sont souvent largement automatisés et industrialisés.
- **Niveau 2** : Il comprend les contrôles permettant, d'une part, de vérifier la validité des contrôles de niveau 1, effectués par les équipes opérationnelles et

d'autre part, de faire le lien avec la maîtrise des risques métiers et stratégiques. Ce palier constitue le niveau des « *contrôles de conformité* ». Il s'agit par exemple de vérifier que les contrôles de droits d'accès sont effectivement menés et suivis de mesures correctives, de conduire des revues des tests PCA (plans de continuité), etc. Le niveau 2 est réalisé par une équipe indépendante des équipes opérationnelles, et idéalement de la filière sécurité (RSSI). Par exemple une cellule « contrôles » rattachée au RSSI, agissant par délégation de la Direction du contrôle interne ou de la Direction de l'audit et des risques.

- **Niveau 3** : Il est en dehors du périmètre du contrôle permanent. C'est-à-dire qu'il intègre les contrôles périodiques diligentés par une entité externe au contrôle permanent (Inspection générale, Contrôle général, etc.). Il comprend également les audits externes. Dans le secteur bancaire où le contrôle est largement développé et réglementé, les trois niveaux existent le plus souvent. Dans d'autres secteurs, les fonctions de niveau 2 et 3 peuvent ne pas être dissociées ou être réalisées par les mêmes équipes.

En dehors des tests d'intrusion ou Pen-Test (Penetration Test), évaluation du plan de migration des applications, contrôle d'accès logique, authentification, etc., les audits de sécurité portent également sur la sécurité physique du SI. En effet, il est plus que vital d'assurer une bonne politique de sécurisation du SI, contre : les défauts d'alimentation électrique, mauvaise climatisation, actes de vandalismes, inondations, incendie et assurer la traçabilité des entrées et le marquage des matériels, etc. La majorité de la sécurité en entreprise est essentiellement axée sur cet aspect, à travers les portes blindées, accès biométriques, agents de gardiennages, etc.

4. La prévention juridique

En plus de l'arsenal technologique et procédural mis en place, les entreprises doivent également avoir recours à des techniques juridiques préventives visant à anticiper, limiter et réduire les dommages subséquents à une atteinte à la sécurité informatique. Les dégâts engendrés par une telle atteinte peuvent être coûteux pour l'entreprise. Toutefois, il est à souligner qu'un sinistre lié à la défaillance de la sécurité d'un système informatique peut ne pas être dû exclusivement à un cybercriminel, un vandal ou à un hacker. La responsabilité peut également être le fait :

- du fournisseur de matériel ou logiciel de sécurité qui n'aurait pas fonctionné,
- du fournisseur d'accès au réseau de télécommunications qui aurait été négligent,
- du fabricant et/ou à l'installateur du réseau informatique de l'entreprise qui aurait mal défini l'architecture et les systèmes de protection,
- d'un préposé de l'entreprise qui aurait commis un acte de malveillance ;
- du chef d'entreprise qui n'aurait pris aucune précaution en matière de sécurité et n'aurait pas protégé ses fichiers stratégiques,
- du fournisseur de logiciels de cryptologie qui n'aurait pas assuré la protection des clés.

L'intelligence juridique[13] se décline comme l'un des facteurs clés de succès de la conception d'une stratégie de sécurité informatique en entreprise. En effet, le droit devient omniprésent dans l'environnement des TIC et acquiert une importance capitale dans la mise en production des systèmes d'information.

Dans le cas d'incidents informatiques, la responsabilité des acteurs qui en assure la gestion est fortement invoquée. Il apparait donc nécessaire que les responsables de la sécurité puissent apporter la preuve que des mesures suffisantes de protection du système d'information et des données ont été mises en œuvre afin de se protéger

[13] Ensemble des règles et méthodes d'intégration du Droit comme outil d'aide à la décision

contre un **délit de manquement à la sécurité** (à défaut d'une obligation de résultat, ils ont une **obligation de moyens**).

Les responsables d'entreprises eux-mêmes doivent être sensibilisés et extrêmement attentifs et à l'égard du cyberdroit **(droit des nouvelles technologies),** afin de s'assurer que leur système d'information est en conformité juridique. En effet, en plus des dispositions réglementaires et légales, ils doivent également être sensibilisés aux contraintes d'une enquête policière. La démarche de sécurité est un processus dynamique qui évolue tout comme les technologies de l'information, et nécessite donc la mise en place d'une veille juridique.

Au regard de tout ce qui suit, il apparait plus qu'impérieux de proposer des garanties sécuritaires, pour les hypothèses ou le sinistre ou l'incident informatique n'a pu être prévenu et évité (défense en profondeur). A ce niveau des dispositions juridiques simples mais efficaces sont à prendre, telles que :

i. ETABLIR DES CLAUSES ET DES ENGAGEMENTS SPECIFIQUES A LA SECURITE DANS LES CONTRATS FOURNISSEURS

Pour des contrats conclus avec les fournisseurs d'informatique, il faut s'assurer que le fournisseur s'engage à garantir au minimum, la mise en place de systèmes de protection (notamment firewall et anti-virus) conformes aux technologies disponibles sur le marché. Enfin, rappelons que pour être efficace, ces engagements devront être valables aussi bien lors de la première livraison du système, que par la suite dans le cadre de la maintenance du système. Il est important de prévoir à la charge du fournisseur une obligation contractuelle de mise à jour régulière du système informatique pour couvrir les cas de défaillance du système de sécurité du fait de son caractère obsolète.

De plus, les contrats de back-up sont une alternative à intégrer dans sa stratégie lorsqu'on s'engage avec un fournisseur. Le contrat de back-up a pour objectif de prévoir les conditions dans lesquelles un fournisseur met à la disposition d'un client

qui se retrouve victime d'un incident l'empêchant de continuer à utiliser son système informatique, un matériel de substitution de configuration équivalente. Généralement pour une période donnée, définie d'accord entre les deux parties et selon les exigences de l'entreprises, ce matériel de substitution permet de continuer l'activité et spécifiquement les opérations clés pour le fonctionnement de l'entreprise.

ii. LES POLICES D'ASSURANCES

Il est aujourd'hui indispensable pour une entreprise d'avoir une police d'assurance qui tienne compte du risque informatique. Les garanties proposées par les assureurs en matière informatique s'articulent autour de trois types de garanties :

- celles relatives au matériel et aux mesures indispensables à prendre pour la poursuite de l'exploitation d'une part, connue sous le nom de "**Tous risques informatiques**" ou "**multirisques informatiques**" (TRI). Ce contrat couvre essentiellement les dommages matériels directs susceptibles d'atteindre les biens de l'assuré, mais il peut également garantir les frais engendrés par la survenance du dommage et les pertes d'exploitation. Cette garantie prend généralement en compte tous les dommages matériels subis par les biens assurés, sous réserve de l'application de quelques exclusions, ce qui se traduit particulièrement dans la rédaction, par une formule type "tout sauf".
- celles relatives aux conséquences pour l'exploitant d'un système informatique de la fraude informatique d'autre part, connue sous le nom de "**Extension des risques informatiques" (ERI**). Ce contrat a pour objet la garantie des pertes de fonds et de biens consécutives à des fraudes, détournements, escroquerie, vol et actes de malveillance ou sabotage immatériel. Ce contrat peut également comporter des extensions de garantie aux pertes d'exploitation consécutives à une perte d'informations ou à l'utilisation non autorisée de ressources informatiques.

- celles relatives à des garanties spécifiques contre le détournement ou encore une assurance concernant les échanges de données informatiques ("EDI")

En somme, ces trois types de garantie peuvent être cumulés et être consignés dans une police unique dite "**Globale Informatique**" (**GI**). Une telle police comporterait l'ensemble des garanties faisant l'objet des contrats examinés ci-dessus à savoir:

- les dommages matériels directs
- les dommages consécutifs à un dommage matériel direct
- les pertes d'exploitation après interruption du service
- les conséquences des fraudes, détournements, escroquerie, vols et actes de malveillance, et éventuellement des extensions comme les agios bancaires.

iii. INTÉGRATION DE LA CHARTE DE SÉCURITÉ DANS LE RÈGLEMENT INTÉRIEUR

Pour être opposable aux salariés de l'entreprise, la Charte doit être adjointe au règlement intérieur dans la mesure où:

- d'une part, elle contient des règles générales et permanentes quant à l'utilisation du matériel professionnel, et
- d'autre part, elle relève de l'hygiène, de la sécurité et de la discipline en entreprise.

Le code du travail Ivoirien stipule en son article **15.1**, chapitre 5 du Titre 1er : « […]*Avant de le mettre en vigueur, le chef d'entreprise doit communiquer le règlement intérieur aux délégués du personnel, s'il en existe, et à l'Inspecteur du*

travail et des lois sociales qui peut exiger le retrait ou la modification des dispositions contraires aux lois et règlements en vigueur.

Les modalités de communication, de dépôt et d'affichage du règlement intérieur, ainsi que le nombre de travailleurs de l'entreprise au-dessus duquel l'existence de ce règlement est obligatoire sont fixées par décret».

Cet article définit les modalités procédurales de modification et de mise en application d'un règlement intérieur au sein de l'entreprise. Toutes les dispositions contenues dans le règlement intérieur sont opposables au salarié de l'entreprise et le manquement aux dispositions dudit règlement entraine la responsabilité du salarié fautif. Le code du travail ivoirien crée à cet effet, des obligations pour l'employé et des droits pour l'employeur, quand il mentionne en son article 41.4 : « *L'employeur ou son représentant doit organiser le contrôle permanent du respect des règles d'hygiène et de sécurité.*

Les salariés, de leur côté, doivent respecter les consignes qui leur sont données, utiliser correctement les dispositifs de salubrité et de sécurité, et s'abstenir de les enlever ou de les modifier sans autorisation de l'employeur ».

L'inobservation des prescriptions ou injonctions émanant du chef d'entreprise, à travers le règlement intérieur par exemple est cause de faute professionnelle. Les fautes selon leur niveau de gravité, pouvant être évoquées par l'employeur sont :

- ***la faute légère ou la faute d'imprudence.***

Il s'agit d'une faute de moindre gravité mais qui fait perdre au salarié, l'indemnité de licenciement (Somme due par l'employeur au salarié licencié hors cas de faute grave ou lourde qui a au moins un an d'ancienneté dans l'entreprise). Cette indemnité est fonction du salaire et de l'ancienneté de l'intéressé et l'indemnité de préavis (l'indemnité compensatrice de préavis est donc égale à la rémunération habituelle du salarié, avantages compris. C'est la somme due par l'employeur qui

dispense le salarié d'exécuter le préavis auquel il a droit en cas de rupture du contrat).

- ***la faute grave***

Cette faute est celle qui rend impossible la continuation du contrat de travail, même pendant la durée de préavis. Elle provoque la rupture immédiate du contrat de travail. Cette faute fait perdre au salarié l'indemnité de licenciement et l'indemnité de préavis.

- ***la faute lourde***

La faute lourde est une faute particulièrement grave, intentionnelle comme le vol, l'injure grave proférée à l'égard de l'employeur sur les lieux du travail et devant témoins et les actes indirects de concurrence. Le travailleur est alors privé de l'indemnité de licenciement, l'indemnité de préavis et l'indemnité compensatrice de congés payés.

Dans la conception de la sécurité informatique en entreprise, les chartes répressives doivent être revues et devenir plus consensuelles, afin d'offrir une alternative aux conventions collectives souvent vides de contenu car trop difficiles à négocier avec les partenaires sociaux. Lorsqu'elles sont annexées au règlement intérieur, les chartes informatiques sont sanctionnées sur le plan disciplinaire. La faute grave peut justifier un licenciement tandis que la faute lourde permet en outre de rechercher la responsabilité civile du salarié pour le préjudice subi. La faute lourde est, en droit du travail Ivoirien, limitée à l'action dolosive (manœuvre entachées d'un dol destinée à tromper autrui pour engager sa responsabilité), destinée à nuire délibérément à l'entreprise.

5. La veille technologique

Avec l'évolution effrénée des technologies et partant des vulnérabilités, Il est vital pour l'entreprise de suivre quotidiennement les dernières mises à jour et failles de sécurité, qui concernent le matériel informatique (serveurs, postes de travail, logiciels, etc.) utilisée dans l'architecture de son système d'information. La veille technologique doit être une tâche entièrement et exclusivement dédiée à un agent ou selon besoin à une équipe, constituée de personnels dotés de connaissance en veille en ligne. Au-delà des outils logiciels de veille en ligne, il est également conseillé de s'inscrire sur les sites spécialisés, s'abonner à des mailing-list, flux RSS, forum spécialisés, etc., pour recevoir ces informations de sécurité. Cette dynamique de veille permet de rester en contact permanent avec les changements qui interviennent sur les systèmes, réseaux, logiciels et de disposer d'une capacité de réaction plus grande, en cas de problèmes majeurs de sécurité.

§4 CHOIX DE L'ENVIRONNEMENT DE SECURITE

L'une des problématiques centrales en matière de sécurité informatique, reste le choix de l'environnement de production du système d'informations. Le traditionnel débat entre les défenseurs du logiciel libre et ceux des logiciels exclusifs, n'a pas encore fini d'alimenter les conversations entre professionnels et experts de la sécurité informatique. Au risque de perdre de vue l'un des principaux enjeux de la sécurisation des SI, ignorer le rôle et la place de plus en plus importante du logiciel libre dans les stratégies de sécurité en entreprise serait préjudiciable pour des entreprises aux ressources limitées. En effet, il est de nos jours rare de trouver des entreprises au sein desquelles le système d'exploitation **LINUX**, réalisation phare de l'école du libre, n'est pas présent quelque part. Même si Linux reste encore très

peu usité pour les travaux de bureautique, force est de constater que l'OS[14] a effectué une incursion spectaculaire dans le domaine du matériel informatique (serveurs web, serveurs d'applications, base de données, poste de travail central, etc.). De plus, tous les grands fournisseurs de matériel l'offrent en option préinstallée, signe de l'acceptation de cette solution comme alternative majeure à la sécurité.

Pour les entreprises en général et celles à ressources limitées en particulier, le logiciel libre présente des avantages indiscutables. Tout d'abord, la ***gratuité*** des applications dans un contexte de crise économique généralisé permet de déployer des solutions d'entreprise viables en évitant les coûts des licences d'utilisation de logiciels. En effet, les coûts d'exploitation et de maintenance des logiciels exclusifs (propriétaires) contraint de nombreuses entreprises à adopter des comportements potentiellement dangereux pour l'intégrité des SI (utilisation de logiciels piratées craqués, version limitées, etc.).

Ensuite, le ***niveau de sécurité*** des applications libres (open source) n'est plus à démontrer. En effet, l'accessibilité au code source de l'application favorise une appropriation du concept mis en jeu dans la création de l'application et partant, un contrôle plus large de la fiabilité et de la sécurité du code. Cette caractéristique est mise en lumière par les communautés d'utilisateurs et de développeurs de logiciels libres aussi compétents que leurs collègues du logiciel exclusif, comme gage de sécurité. A titre d'exemple, plusieurs algorithmes open source sont présentement très utilisés dans les solutions de cryptage, tels que : OpenSSH, 3DES Blowfish, AES et Arcfour. En outre même le géant Google, a lancé à son tour un outil de chiffrement open source baptisé KeyCzar. S'appuyant sur les bibliothèques OpenSSL, PyCrypto et Java JCE, cet algorithme serait censé aider les développeurs à utiliser des technologies de chiffrement sûres pour leurs applications.

[14] Operating System ou système d'exploitation. Programme informatique permettant l'exploitation proprement dite d'un périphérique informatique ou TIC (smartphone, PC, etc.). Les plus célèbres sont Windows, LINUX, UNIX, Debian, etc.

De plus, les logiciels libres présentent une ***forte flexibilité*** et une ***adaptabilité***. En effet, les logiciels open source peuvent être modifiés et adaptés pour répondre à des exigences spécifiques d'une organisation. Cette caractéristique offre la possibilité aux organisations de disposer d'un outil épousant complètement les réalités et attentes du système d'information, contrairement aux logiciels exclusifs. L'entreprise adapte le logiciel à ses attentes dans le cadre du libre et garde le contrôle de sa stratégie de développement dans le cas du libre, tandis qu'elle contrainte de s'adapter à la stratégie de développement de l'éditeur de logiciel exclusif. Cet état de fait pose le problème des rythmes de changement de l'environnement de production, qui reste relativement supportable pour des entreprises plus puissantes.

Enfin, tous ces avantages ne sauraient occulter les risques liés à l'utilisation de logiciels libres. Notamment en ce qui concerne la fourniture de services de soutien professionnels à la mise en œuvre des solutions. Le risque de dépendance à un outil non soutenu, d'être confronté à des bogues sur des solutions hébergeant des services critiques pour l'entreprise, n'est pas à négliger. Cependant, de nombreux logiciels open source bénéficient de services de soutien non gratuits (payants) généralement assurés par des organisations ou entreprises à but lucratif, qui se construisent le modèle économique autour du projet d'élaboration du logiciel libre en question.

Plusieurs logiciels open source sont commercialisés selon un modèle de double licence, à savoir : une version soutenue par la communauté est disponible sous licence d'exploitation libre et une version soutenue par un revendeur est commercialisée sous licence d'exploitation commerciale. Le système d'exploitation Solaris de Sun, en est une des nombreuses illustrations. Ce modèle de suivi du logiciel propose en fin de compte un double niveau de soutien, qui renforce la capacité de réactivité en cas de failles de sécurité.

En résumé, la solution la plus adaptée semble reposer dans l'établissement d'un compromis judicieux entre logiciel exclusif et libre. Le logiciel libre présente un avantage considérable pour les entreprises à ressources limités, mais il convient

d'élaborer des plans de secours, s'appuyant sur des outils stratégiques anticipatifs. Il s'agit par exemple d'évaluer les actifs reposant sur des logiciels libres et prévoir des plans de remplaçant ou l'utilisation de ressources internes (humaines, techniques, logiciels propriétaires). Une solution libre, bien diffusée et largement soutenue par une large collectivité, peux constituer un choix viable si les fonctionnalités répondent aux besoins de l'entreprise. A l'heure de l'émergence des outils libres, les entreprises qui n'intègrent pas le logiciel libre dans leurs stratégies de sécurité SI, prennent le risque d'être à la traîne en termes de compétitivité.

Quelques logiciels libres appliqués à la sécurité infrmatique

- ***Nmap*** : Permet le balayage automatisé des ports TCP et UDP d'un système distant Nmap -sS -v -P0 -g 53 -p- –-data-length 128 -T INSANE -sV -O -f –oN ./résultat.txt 192.168.0.0-255
- ***Wireshark*** : Outil d'écoute de réseau
- ***Nessus*** : Outil de balayage des vulnérabilités
- ***Netcat*** : Permet de générer des connexions UDP et TCP
- ***Snort*** : Permet de détecter les intrusions
- ***OpenSSH*** : Permet de se brancher à d'autres ordinateurs sans mots de passe
- ***OpenSSL*** : Protocole d'encapsulation sécuritaire
- ***John the Ripper*** : Attaque des mots de passe par force brute ou dictionnaires
- ***VNC*** : Connexion distance facile et légère
- ***Iptables*** : Permet de tout bloquer
- ***SpamAssasin*** : Anti-pourriel
- ***ClamAv*** : Anti-virus gratuit
- ***Firefox*** : Plug-ins qui font une partie du travail
- ***Dig*** : Permet d'interroger un service DNS avancé
- ***NsLookUp*** : Permet d'interroger un service DNS
- ***Traceroute*** : Permet de découvrir des réseaux
- ***Ping*** : Vérification de la présence d'un système
- ***NbtStat*** : Affiche les statistiques du protocole NetBios
- ***DBAN*** : Supprime les informations sur les disques
- ***GPG*** : Permet le chiffrement
- ***TrueCrypt*** : Permet le chiffrement du disque dur
- ***NetStumbler*** : Permet de détecter les réseaux sans-fils

- ***ToneLoc*** : Balayage des lignes téléphoniques pour les modems
- ***SeLinux*** : Permet d'analyser les actions prisent par les utilisateurs
- ***Kismet*** : Outil d'écoute réseau sans-fils
- ***TripWire*** : Gestion des changements sur les systèmes
- ***Nikto*** : Outil automatisé des services Web
- ***JMeter*** : Permet de tester le comportement d'un système Web Apache
- ***IDSWakeUp*** : Permet de tester la fiabilité d'un système de détection d'intrusion
- ***DSNIF*** : Permet d'écouter et de capturer les informations communiquées entre deux postes réseaux
- ***Achilles*** : Permet d'intercepter et de modifier les requêtes http(s)
- ***TsCrack*** : Attaque par force brute d'un service de bureau distant
- ***Stunnel*** : Permet d'établir un tunnel SSL
- ***Packit*** : Outil de création de paquet
- ***PFSense*** : http://www.pfsense.com/
- Outils de chiffrement pour linux :
  - http://linuxhelp.blogspot.com/2006/08/disk-encryption-tools-for-linux-and.
- Alternative Linux :
  - http://www.linuxalt.com/
  - http://www.econsultant.com/i-want-open-source-software/
  - http://www.damicon.com/resources/opensoftware.html
- Test de performance Apache Jmeter: http://jakarta.apache.org/jmeter/
- IDS WakeUP: http://www.hsc.fr/ressources/outils/idswakeup/
- MetaSploit : http://www.metasploit.org/

En résume, la conception de la sécurité informatique en entreprise, revient à développer une culture profonde de la sécurité en entreprise, pour ensuite créer des liens organisationnels fonctionnels entre les acteurs et la politique de sécurité. Ceci revient à :

- Savoir inscrire la démarche sécurité dans la durée et le long terme
- Valoriser les progrès accomplis
- Reconnaitre et écouter les pratiques de terrain afin de conserver les acquis
- Savoir faire vivre les procédures établies en partageant les expériences et en les mettant à jours en fonction de l'évolution de l'entreprise

- Mettre en place un système de gestion des compétences et de formation performant (recruter du personnel qualifié aux postes de sécurité, initier tout les employés à la culture de sécurité informatique, quelque soit les domaines de compétence)
- Savoir faire partager les bonnes pratiques, retour d'expérience (interne), benchmarking (externe)
- Promouvoir une vision intégrée de la sécurité (aller au delà des aspects techniques de la sécurité informatique et prendre en compte les aspects organisationnels, humains, etc.)
- Instaurer un dialogue permanent entre les parties

TROISIEME PARTIE

RSSI, RM :

LES NOUVEAUX METIERS DE LA SECURITE DES SYSTEMES D'INFORMATIONS

1 QUI EST LE RSSI?

L'importance capitale qu'a acquise la sécurité des systèmes d'informations, a nécessité une réorganisation et une redéfinition des concepts de bases du secteur de la sécurité. En effet, si les budgets et autres dépenses liées à la sécurité restent encore très faibles comparativement à d'autres secteurs, il convient de noter que les métiers de sécurité informatique tendent à se professionnaliser et à acquérir une plus grande importance dans les stratégies des entreprises. Si le comptable (secteur financier) est le responsable de la santé financière de l'entreprise, le Responsable de la Sécurité des Systèmes d'Information (RSSI) est lui, le comptable de la santé informatique de l'entreprise.

§1 ROLE DU RSSI

Le RSSI est celui qui est chargé de la définition et de la mise en œuvre de la politique de sécurité de l'entreprise. Il possède en outre un rôle stratégique d'information, de conseil et d'alerte de la direction générale sur les risques en matière de sécurité informatique.

La fonction de RSSI est essentiellement managériale et consiste à encadrer une équipe d'ingénieurs et de techniciens d'exploitation, dont il organise et contrôle le travail. Selon le **CIGREF**[15], « *le RSSI assure un rôle de conseil, d'assistance, d'information et de préconisation. Il peut intervenir sur tout ou partie des systèmes informatiques et télécoms de son entreprise. Il effectue un travail de veille*

[15] Club Informatique des Grandes Entreprises Françaises

technologique et réglementaire sur son domaine et propose des évolutions qu'il juge nécessaires pour garantir la sécurité logique, physique, etc., du système d'information dans son ensemble. Il est l'interface reconnue des exploitants et des chefs de projet, mais aussi des experts et des intervenants extérieurs pour les questions de sécurité de tout ou partie du système d'Information ».

Dans les faits, son rôle va plus loin. En effet, il est chargé de l'évaluation et de la gestion des risques liés au SI. Il assure dans ce contexte, une fonction transverse de manager :

- en rassemblant de nombreux contributeurs (à la communication, aux ressources humaines, à la stratégie, au juridique, au contrôle interne, à l'audit, etc.)
- en dialoguant avec les directions métier et la direction des systèmes d'information sur les objectifs de sécurité à définir, les référentiels de sécurité à appliquer, les parades à mettre en place
- en définissant les exigences attendues en matière de sécurité.

Face à la complexité accrue des systèmes d'informations et des technologies de l'information utilisées, face aux exigences réglementaires et face à la démultiplication des prestations d'infogérance et d'externalisation, le RSSI est obligé de considérer le système d'information dans sa globalité. Pour ce faire, il doit nécessairement s'entourer d'experts techniques (ingénieurs système, réseaux, développement, juristes, marketing, etc.), afin de prendre en compte tous les aspects ayant trait à la gestion opérationnelle des risques sous sa responsabilité.
En sa qualité de responsable de la gestion des risques liés aux SI, la fonction de **RSSI** nécessite plus que jamais son implication directe dans la définition et la gestion des actions de sécurisation. Celle-ci doit se traduire par sa participation active aux différentes phases du processus de gestion des risques (identification des risques, plan d'action de réduction et de contrôle, évaluation des contre-mesures mises en place).

§2 MISSIONS DU RSSI

Les principaux objectifs du RSSI sont les suivants :

I. *Prévenir les risques dès les phases de développement des projets* : conseiller en amont les maîtres d'œuvre et maîtres d'ouvrages sur tous les nouveaux projets, en y intégrant une dimension sécurité. Le RSSI s'assure de la prise en compte des exigences de sécurité et valide ces exigences dans les cahiers des charges des projets sensibles

- *Proposer des plans d'actions de réduction et de contrôle* : le RSSI propose des actions et présente les moyens à mettre en œuvre pour garantir un niveau de risque acceptable et accepté par l'entreprise. Pour ce faire, il met en place et pilote les comités de contrôle et de pilotage de la sécurité
- *Obtenir des décisions vis-à-vis des plans d'action* : Suivre la mise en place des plans d'actions décidés : le RSSI vérifie que les solutions mises en place répondent aux contraintes sécuritaires et sont conformes aux cahiers des charges. Le RSSI définit et met en place des bases d'incidents
- *Rendre compte à la Direction générale et communiquer sur la sécurité des SI, avec la direction des systèmes d'information* : Le RSSI définit et propose la politique de sécurité afin de la faire approuver par la Direction Générale
- *Sensibiliser toutes les équipes à la sécurité des systèmes d'information* : Le RSSI définit les référentiels de sécurité de l'entreprise et notamment ceux relatifs aux bonnes pratiques

§3 POSITIONNEMENT AU SEIN DE L'ENTREPRISE

Dans de nombreuses grandes entreprises, le RSSI est rattaché au directeur des systèmes d'information (DSI). Dans les entreprises moins "puissantes", le rôle de RSSI n'est pas très clairement établit et il est très souvent confié à un agent disposant de connaissance en informatique, le plus souvent relié au Directeur

Informatique. La tendance est plutôt à la désignation d'un agent disposant de connaissances générales en informatique et dans les divers domaines touchés par les exigences de la sécurité informatique (juridique, marketing, ressources humaines, etc.).

Dans les grandes entreprises, le département sécurité des systèmes d'informations est autonome et indépendant de la Direction informatique. Dans ce genre d'entreprise, la Direction Générale délègue au RSSI la responsabilité de coordonner la mise en œuvre et le contrôle de la politique de sécurité des SI à tous les échelons et domaines de l'entreprise et ce, sous la responsabilité hiérarchique de la Direction des systèmes d'information.

§4 DEVENIR RSSI

A priori, la fonction de RSSI est destinée aux professionnels du domaine de l'informatique, impliqués dans la sécurité au sein de l'entreprise. Mais en pratique, la fonction de RSSI est accessible à toute personne possédant des connaissances en matière de réseaux et d'informatique, souhaitant approfondir leurs connaissances en matière de management de la sécurité.

Si la maîtrise du savoir faire technologique est un plus, le RSSI doit posséder des savoirs faire généraux primordiaux, tels que la compréhension de l'environnement et du fonctionnement de l'entreprise, la connaissance des clients de la DSI (activités et besoins), et des aptitudes comportementales essentielles comme la rigueur, le sens de la méthode et de la probité, ainsi que des talents de communicateur et d'organisateur, afin de concilier au mieux les interventions des experts techniques (informaticiens, juristes, etc.) dans la réalisation des objectifs liés à la sécurité.

Aussi, une bonne connaissance des normes de référentiels de sécurité : ISO 15408, La famille des normes ISO 27000, ITIL/Cobit, PCI/DSS, BS7789-2, etc. est-elle d'une importance capitale.

Notons qu'il n'existe pas à l'heure qu'il est, de diplôme spécifique à cette fonction, mais des certifications françaises et Européennes naissent très

progressivement. Toutefois, un DESS en sécurité des systèmes d'information est disponible à l'Université des Technologies de Troyes en FRANCE. Si le métier de RSSI a acquis dans les grandes organisations une reconnaissance de la part des professionnels, il peine encore à s'installer dans les entreprises évoluant dans des écosystèmes IT moins évolués.

2 RISK MANAGER (RM) ET RSSI : DEUX FONCTIONS COMPLEMENTAIRES

§1 *LA FONCTION RISK MANAGER (RM OU MANAGER DE RISQUES)*

D'origine anglo-saxonne, ce métier s'est implanté progressivement en France depuis les années 70, notamment avec les activités industrielles à hauts risques : chimie, pétrole, explosifs, etc. Généralement le Risk manager gère la politique et le plan d'assurance de l'entreprise. Selon les cas, il peut éclairer la direction générale sur les risques majeurs encourus (risques stratégiques, opérationnels, potentiels et avérés), leur niveau de maîtrise et la façon dont sont traités les risques résiduels (solutions de financement sur fonds propres à travers le recours aux assurances et autres solutions alternatives de financement).

Dans certaines entreprises, il est le moteur des dynamiques d'analyse globales des risques et d'accompagnement des mesures globales d'accompagnement. Dans le secteur bancaire par exemple, les accords de Bâle 2, sur la gestion des risques opérationnels, offrent des éléments de cadrage particulièrement pertinents. Ces principales missions sont de :

- Concevoir des outils et méthodes de gestion des risques,
- Elaborer et mettre en œuvre la politique et le plan d'assurance de l'entreprise,

- Conseiller les métiers sur les mesures de prévention, protection, détection et réaction à un risque,
- Communiquer sur les risques avec la direction générale.

Il a un rôle très important, en ce sens qu'il doit maintenir les réseaux de veille et d'alertes, convaincre et fédérer le milieu professionnel, gérer les incidents et les crises, négocier les contrats d'assurance, gérer les flux financiers et diffuser la culture de la sécurité dans toutes se composantes. Très souvent rattaché aux directions juridiques ou financières, il serait idéal que le Risk Manager soit directement rattaché à la Direction Générale, vu son rôle stratégique majeur.

S'ils ne sont pas les seuls acteurs en charge de la gestion des risques, le RM et le RSSI sont en revanche les seuls garants de l'identification des risques liés au Système d'information et de la mise en œuvre des moyens pour contrôler et gérer ces risques.

Le RM ne disposant très souvent pas d'une expertise SI, s'appuie sur les travaux et actions menées par le RSSI, pour identifier et participer à la maîtrise des risques. Par ailleurs, le RSSI s'appuiera sur les travaux du RM, pour définir les priorités et le niveau des contre-mesures à mettre en place en fonction des solutions de financement des risques résiduels envisageables.

§2 ATTENTES ET APPORTS RECIPROQUES ENTRE RM ET RSSI

Une des grandes difficultés du RSSI est de proposer des actions de réduction et de contrôle des risques en adéquation avec les enjeux de l'entreprise et complémentaires aux solutions de financement des risques résiduels envisageables. En effet, pour être efficace, la sécurité des Si doit répondre de manière proportionnée à la couverture de chaque risque identifié et non-accepté. De ce point de vue, un travail commun avec le RM est nécessaire pour structurer la démarche de maîtrise des risques de façon à ajuster en conséquence, les montants à garantir et si

nécessaire, concevoir des solutions alternatives de financement du risque résiduel (récupération).

De l'autre côté, le RM dans sa fonction de manageur du risque se trouve confronté à des difficultés considérables. D'une part, tous les risques identifiés ne sont assurables, d'autre part les risques assurables, ne le sont qu'en partie dans la pratiques, en tenant compte des franchises dans les contrats (disposition prévue dans un contrat d'assurance, traduit par une somme d'argent à la charge de l'assuré en cas de survenu d'un sinistre).

Pour lever toutes ces difficultés, le RM doit disposer des informations qui lui permettront de traiter le risque en amont et non en aval, lorsqu'il s'agit de régler un préjudice. Il s'agit pour le RM d'établir un langage commun en adéquation avec les enjeux et objectifs de l'entreprise de façon à écarter autant que faire se peut tout risque de contentieux entre l'assureur et l'assuré au moment de la survenu d'un sinistre.

L'analyse de l'interaction entre le RM et le RSSI traduit la nécessité d'établir un véritable dialogue entre ces deux fonctions. Bien que ces deux fonctions stratégiques soit distinctes par les méthodologies et les outils de travail, elles poursuivent les mêmes objectifs, à savoir la maîtrise du risque et l'assurance d'un niveau de sécurité accepté par l'entreprise, en considération de sa culture, ses objectifs. Toutefois, il est à noter que la tendance est plutôt à un jumelage de ses fonctions. En effet, les entreprises tendent à confier l'essentiel de ses missions et tâches à des entités uniques, ce qui augmente les risques de défaillance graves dans la sécurité en général, et dans la sécurité des SI en particulier.

3 NOUVEAUX DEFIS DU RSSI EN ENTREPRISE

En 2012, les attaques dirigées contre les PME ont représenté près du tiers des actions (31%) et le nombre des cyberattaques ciblées a augmenté de 42 % dans le monde, selon un rapport de la société américaine de sécurité informatique ***SYMANTEC***.

Les attaques de plus en plus complexes et astucieuses, face à une technologie dynamique et des utilisateurs de plus en plus dépendants, soulignent d'un double trait la nécessité de proposer des stratégies globales et cohérentes.

En plus des menaces classiques de sécurité informatique, le développement de l'Internet embraqué et la virtualisation de l'informatique ont rajouté une couche de difficulté à la mission des responsables de la sécurité des systèmes d'information. A l'ère du web 2.0 et de l'Internet à très haut débit, les challenges que doivent affronter les professionnels de la sécurité informatiques sont énormes.

§1 *LE SOCIAL ENGINEERING*

Le social engineering ou « ingénierie sociale » est une forme de cybercriminalité qui a pour but d'obtenir de la part de sa victime, qu'elle réalise une action que vous lui dictez de faire (effectuer un virement bancaire, désactiver un antivirus, formater un serveur, ouvrir une pièce jointe, etc.) ou vous remettre volontairement des informations sensibles auxquelles vous n'êtes pas censé avoir légitimement accès

(mot de passe, code d'accès, etc.). Cette technique s'appuie sur la manipulation et la force de persuasion, afin d'acquérir de façon déloyale une information ou une la réalisation d'une action.

Utilisant ses connaissances et les renseignements dont il dispose sur la cible, le hacker abuse de la confiance, de l'ignorance ou de la crédulité de ses victimes pour parvenir à ses fins malveillantes.

L'amélioration des techniques de sécurisation des SI entraine pour les pirates, une augmentation du niveau de difficulté des attaques ciblant les serveurs, donc une diminution de la rentabilité de celles-ci. Les experts en sécurité informatiques constatent que les pirates se sont tournés ces derniers mois, vers le poste de l'utilisateur à l'intérieur de l'entreprise. Ainsi pour atteindre une grande entreprise qui travaille avec des sous-traitants, le moins périlleux pour l'attaquant sera de tenter de gagner un accès sur le poste de travail d'un utilisateur de la PME, afin d'exploiter le facteur confiance pour accéder aux serveurs de la grande entreprise

De plus, les variations et techniques connexes ne cessent de grandir, notamment le « phishing » et sa variante le « spear phishing ».

Les attaques de type phishing sont désormais ciblées et personnalisées, afin d'avoir un impact certains sur des utilisateurs peu aguerris en matière de sécurité. Dans le cas où l'administrateur réseau par exemple est visé, l'ensemble du personnel non-technique avec qui il entretient des liens étroits de travail au sein de l'entreprise, constitue une cible de choix pour l'attaquant.

En outre, une des dernières tendances en matière de cybercriminalité astucieuse, est la fameuse attaque dite « *whater hole* » ou trou d'eau. Cette attaque consiste à traquer les hobbies et habitudes de navigation (sites web les plus visités, sites de divertissement) d'un agent, afin de s'introduire dans le système de l'entreprise par son biais. L'attaquant étudie et répertorie les hobbies de sa cible, avant de piéger les sites web auxquelles elle a régulièrement accès (jeux, chat, divertissement, etc.). Ensuite il peut aisément prendre le contrôle de la machine de sa victime en utilisant des scripts malveillants.

Notons que le but de ces attaques n'est pas toujours de voler des informations personnelles ou sensibles, mais elles peuvent également servir à prendre le contrôle

des infrastructures informatiques d'une entreprise, afin de réaliser des attaques contre d'autres entreprises (PC-Zombies dans des réseaux de BOTNET).

§2 LE BYOD (BRING YOUR OWN DEVICE)

Le **BYOD** (bring your own device ou « Apportez Votre Propre périphérique ») est une pratique qui consiste pour l'employé à utiliser ses équipements personnels (Smartphone, ordinateurs portables, etc.) dans le cadre de la réalisation de ses tâches professionnelles. C'est une tendance généralisée dans le monde de l'entreprise est d'autant plus accentuée dans les PME, au sein desquelles plus de 65% des salariés auraient recours en France.

Cette tendance est soutenue par les exigences de sécurité auxquelles les responsables de la sécurité des systèmes d'informations doivent faire face et les exigences budgétaires y associées. En effet, on demande très souvent aux DSI et RSSI d'assurer un niveau élevé de sécurité avec des moyens très limités, ce qui a pour effet de conduire ces responsables sécurité à se tourner vers de nouvelles alternatives. Le BYOD assure indéniablement une réduction des coûts des investissements en équipements et comporte bien d'autres avantages, qui ne sauraient pour autant occulter les risques énormes de sécurité y associés.

Le BYOD fait référence à tout type d'équipements physiques personnels (Smartphone, tablettes, blackberry, etc.), mais aussi à des services hébergés dans le Cloud. Le BYOD, bien maitrisé et bien encadré peut permettre une réduction des dépenses et une maximisation de la productivité et des revenus.

Les risques de sécurité dans un système de BYOD implémenté sans une stratégie cohérente avec les objectifs de l'entreprise, constitue un risque « mortel » pour l'entreprise.

Une fois de plus, la solution réside dans la mise en place d'une stratégie concertée, basée sur le bon vouloir des employés d'utiliser leurs équipements personnels dans le respect des règles définies et l'adhésion totale à la politique de sécurité de l'entreprise.

§3 LA SENSIBILISATION EN ENTREPRISE

Processus évolutif et stratégique pour l'entreprise, la sensibilisation a pour fin de modifier les regards, la perception et partant, les comportements des individus en ce qui concerne des enjeux distincts liés à l'actualité de chaque organisation. Il peut s'agir de la promotion du développement durable, projet de changement (déménagement, nouvelle organisation, etc.), meilleure insertion des personnes handicapées dans l'entreprise, promotion de la parité, sécurité de l'information, bien-être au travail, etc.

Une sensibilisation efficace se doit d'être basée sur le long et moyen terme, afin de favoriser un changement habitudes, de comportements, de croyances, de convictions, etc. Pour ce faire, la sensibilisation doit être considérée comme un véritable projet stratégique de développement, c'est-à-dire : bénéficier d'un financement (budget prévisionnel), d'une stratégie intégrée et de moyens de contrôle de l'efficacité.

Un personnel sensibilisé est un personnel qui a reçu des informations, les a intégrés en fonction de sa propre sensibilité et ses aptitudes intellectuelles. L'objectif lorsque l'on entreprend une démarche de sensibilisation, est d'arriver à faire évoluer la culture individuelle et collective susceptible de produire le changement escompté. Globalement la sensibilisation est un effort de **recadrage**.

Selon les travaux du Dr. KOURILISKY Françoise, Docteur en psychologie et diplômée de Sciences Politiques, le processus de sensibilisation doit respecter les trois étapes suivantes :

- Etape 1 : Le **recadrage de point de vue** en premier lieu car nous ne percevons la réalité qu'au travers de nos points de vue, de nos grilles de compréhension ; cette perception est donc forcément partielle et partiale. En ce sens, des actions de sensibilisation impliquant des personnages mis en situation pourront accompagner cette étape où il faut que chacun puisse déplacer son propre point de vue. En ce sens,

des médias combinés en un parcours ou en supports de communications aideront chacun à s'imaginer ou au contraire, à s'opposer aux actions et décisions des personnages mis en scène.

- Etape 2 : Le **recadrage de sens** qui permet, sur des sujets et/ou faits identiques, de proposer une nouvelle interprétation, un sens nouveau. Par exemple, il s'avère difficile de sensibiliser sur la sécurité de l'information au sein des entreprises car les comportements attendus sont souvent « interprétés » comme des freins, des contraintes. Une action de sensibilisation sur les mêmes sujets mais portant sur les risques personnels quant à la sécurité des informations permettra de fournir d'autres types d'interprétations qui apporteront un sens nouveau et des éléments d'acceptation de l'élan de sensibilisation.

- Etape 3 **:** Le **recadrage de comportement**. Cette dernière étape insiste sur le fait que l'explication, seule, n'est pas une condition suffisante pour *changer*. La raison principale en est que le comportement résulte d'une certaine cohérence entre la personne qui le produit et sa vision du monde, de la situation. On agit généralement dans le sens de nos croyances, pas à l'encontre de celles-ci et malgré les risques que cela peut nous faire courir (sanctions professionnelles, risques liés à la santé etc.).

Figure 4: Processus de sensibilisation

4 QUELQUES METHODES ET OUTILS D'ORIENTATION DE LA SECURISATION DE L'INFORMATION EN ENTREPRISE

En amont de toute tentative de proposition de stratégie de sécurisation de l'information en entreprise, un diagnostic basé sur des objectifs clés tenant compte de la spécificité de l'entreprise doit être établi. Les questions principales que les responsables de la sécurité informatique en tant que processus intégré au sein de l'entreprise, devraient se poser dans l'élaboration des mesures de sécurité informatique sont les suivantes :

- Qu'est-ce qui est critique pour mon entreprise en termes d'infrastructure?
- Mon entreprise est-elle bien outillée en termes de sécurité de l'information?
- Mon SI assure-t-il la pérennité, la confidentialité, l'intégrité des mes données sensibles?
- Quels sont les enjeux de la protection de mes données sensibles ?
- L'environnement interne est-il bien maîtrisé ?
- Mes collaborateurs adhèrent-ils au projet sécurité SI de l'entreprise ?
- Les ressources allouées sont elles cohérentes avec mes objectifs de sécurité ?

De nos jours, **l'information** est au cœur du développement des entreprises. En effet, elle a acquis une importance capitale, puisqu'elle représente une valeur marchande considérable et incontestable. L'information constitue aujourd'hui ***le nerf de la guerre économique***.

Au delà des définitions purement techniques, faire de la sécurité informatique revient dans un sens à protéger les informations que contiennent les systèmes d'information. Car en vérité, quand on perd un ordinateur portable, ou téléphone mobile (PDA, Smartphone, etc.) ou tout autre device, ce n'est pas le matériel en lui même qui représente la plus grosse perte, mais plutôt les données qu'il contient. L'on aurait plus de mal a évaluer la valeur marchande des actifs informationnels de son entreprise, que celle du matériel. De ce fait, il convient d'assurer une protection maximale de l'information au sein de l'entreprise.

De manière générale, l'on distingue au sein de l'entreprise, deux catégories d'informations:

- les informations publiques
- les informations privées (internes).

Cette section présente un ramassis de techniques et stratégies qui adaptées au contexte de l'entreprise pourraient constituer des éléments clés de la stratégie de sécurisation de l'information.

§1 PROTEGER LES INFORMATIONS PUBLIQUES

1. Achats sécurisés :

Les webmasters ou les personnes ayant créés la page web doivent disposer d'un cryptage sécurisé (du type https://www.nomdusite.ci) pour que des renifleurs ne puissent pas obtenir eux aussi les données du client en train d'effectuer une transaction. Cette mention est très importante quand il s'agit d'utiliser des sites où

l'on vous demande des données confidentielles (mot de passe, numéro de carte de crédit, etc.). Par exemple sur les pages de e-banking ou de réseaux sociaux (Facebook, Twitter, etc.) ou pour votre compte de messagerie interne. Aujourd'hui pratiquement tous les sites necessitant la communiction d'informations sensibles utilisent des protocoles de chiffrement tels SSL/TLS.

Les webmasters doivent utiliser des clés de chiffrement ayant une longueur supérieure ou égale à 80 bits, plus difficile à craquer. Utiliser un navigateur qui supporte le 128 bits. Ne pas hésiter pour les groupes ne disposant pas de grands moyens techniques et financiers, à recourir aux intermédiaires financiers (banques, plateforme de e-commerce, etc.)

En résumé, il n'y a point de salut sans le protocole SSL (Secure Socket Layer), utilisé pour sécuriser les transactions.

2. Sauvegarde des données

Sauvegarder les données est capitale pour une entreprise, quelle que soit sa taille, du moment où une information importante pour l'entreprise est stockée dans son système d'information. Les professionnel de la sécurité s'efforcent à garantir un niveau de sécurité satisfaisant, mais il n'est pas exclu que des failles (risques logiques, risques physiques) puissent exister, susceptible d'entrainer la perte des données de l'entreprise.

Effectuer des partitions dans votre disque dur et sauvegarder les données de votre site web, par des mécanismes de backup. De plus, assurez-vous que vos données soient uniquement en mode lecture sur le Net. La fréquence des sauvegardes dépend de la quantité de données que vous acceptez de perdre en cas de destruction de vos données.

Prévoir des règles de stockage physiques très pointues, afin de conserver les sauvegardes physiques (disk dur, Cd, ect.) loin des ordinateurs qui contiennent les données originales.

Dans le cas de données chiffrées, il faut également penser à sauvegarder les clés de chiffrement, afin de pouvoir accéder aux données sauvegardées.

Il est conseillé de procéder à une sauvegarde automatique au delà de 10 utilisateurs.

En somme trois alternatives s'offrent aux entreprises, à savoir :

- **Sauvegarde sur PC et disques externes**

Elle a l'avantage de pouvoir être réalisée de n' importe où, quand l'on dispose de matériel portable, mais demande beaucoup plus de temps.

- **Sauvegarde sur un serveur entreprise**

Les risques de perte de fichiers sont considérablement réduits avec l'utilisation d'un serveur entreprise. Les sauvegardes y sont automatiques et sécurisée, mais les risques de décalages de temps peuvent entrainer des pertes de données.

- **Télé-sauvegarde des données**

Un serveur distant installé chez le prestataire de service de télé-sauvegarde de données, effectue automatiquement la sauvegarde de vos données. Cette alternative présente l'avantage de ne nécessiter aucune intervention technique du client et propose un grand volume de stockage. Cependant les couts de souscription à ces services peuvent être très énormes et la sauvegarde dépend exclusivement de la disponibilité de la connexion à Internet.

- *Amanda (Unix, Windows)*
- *Atempo Time Navigator*
- *EMC Networker*
- *HP Data Protector*
- *Veritas NetBackup DataCenter*
- *IBM TSM (Tivoli System Management)*
- *Rsync*
- *RAID*
- *Mtree*

Pour aller plus loin :

http://www.telechargercours.com/securite/la-sauvegarde-des-donnees-integrite-et-disponibilite-du-systeme-informatique/

http://www.freebsd.org/doc/fr_FR.ISO8859-

3. Utilisation de la carte bancaire

Avec le développement des TIC et le taux de pénétration d'Internet dans nos pays Africains, l'imminence de l'explosion du commerce électronique se fait grandissante. Si vous effectuez des achats ou toute autre transaction par carte bancaire, il faut s'assurer que cette dernière n'a pas été volée ou falsifiée, d'où la nécessité de se procurer ces cartes auprès de fournisseurs agréés.

Vérifiez également l'authenticité des sites sur lesquels vous effectuez des transactions, en saisissant directement l'adresse url du site dans la barre d'adresse, afin d'éviter les attaques par Phishing. Entre autres, ne divulguez jamais votre mot de passe et conservez le jalousement, de sorte à n'être que le seul à zn avoir connaissance.

4. Les annonces publicitaires

De nombreuses entreprises par le biais des webmasters et autres personnels du département marketing commettent souvent l'erreur de publier des informations sensibles, à des fins commerciales. Citer par exemple dans des annonces publicitaires, la version du système d'exploitation utilisé sur le serveur de votre entreprise, les logiciels et progiciels utilisés en interne, les protocoles de chiffrements spécifiques, la qualité du materiel, etc. ; dans le but d'augmenter la confiance des partenaires et clients de votre entreprises, peut constituer une faille exploitable par des cybercriminels. Publier de telles informations facilite la phase la plus difficile de toute attaque informatique, à savoir le footprinting (collecte d'informations).

Des cybercriminels qui désirent obtenir illicitement vos données, pourront se servir de telles informations pour mener des attaques pour le social engineering ou par analogies en exploitant des techniques connues sur le matériel que vous utilisez.

Il faut trouver un compromis entre les objectifs de vente du marketing et les objectifs de sécurité de la DSI.

5. Les Spams

L'entreprise doit laisser le choix aux clients de signaler clairement s'ils souhaitent recevoir de façon périodique (chaque semaine ou mois…) un catalogue de ses offres ou toutes sortes de publicité. Car les spams, dans tous les autres pays dotés d'une législation en la matière, sont illégaux et passibles de poursuites judiciaires. La tendance en la matière dans les législations en cours en Côte d'Ivoire et dans les pays d'Afrique devrait suivre cette dynamique. Une des techniques anti-spam consiste à publier son adresse e-mail dans des fichiers images publiés dans les pages web. Ainsi les robots utilisés par certains spammeurs n'indexeront pas votre adresse électronique, réduisant du coup les risques d'être spammé. Sinon des solutions techniques spécifiques existent, tels que : **SpamAssassin** : anti-pourriel open source, etc .

§2 PROTEGER LES INFORMATIONS PRIVEES (INTERNES)

1. Création de badges de couleurs différentes

La création de badges de couleurs différentes, munis de grandes photographies, permet de distinguer les salariés des services, les stagiaires, les sous-traitants, les fournisseurs, les partenaires commerciaux et les autres visiteurs. Cette stratégie vise à renforcer la sécurité physique du système d'exploitation, car s'il est techniquement périlleux de « *faire tomber* » un serveur bien protégé, il en est moins difficile d'en rompre l'alimentation électrique par exemple.

2. Création et gestion de mots de passe complexes

La création d'une stratégie de mots de passe complexes pour le service informatique va permettre d'utiliser une série de combinaisons de majuscules, de minuscules et de numéros. Il est conseillé de suivre les règles suivantes :

i. La taille du mot de passe ne doit pas être inférieure à 8 caractères
ii. Le mot de passe ne doit figurer sur aucune liste de mots de passe dits classiques (12345, password, motdepasse, etc.),
iii. Le mot de passe ne doit pas être un mot du dictionnaire, car il pourrait être cracké en utilisant la technique dite de brute force
iv. La durée de validité du mot de passe doit être limitée pour les accès aux comptes d'entreprises (messagerie, etc.), afin de s'assurer que les mots de passe seront régulièrement changés

Ces différentes exigences doivent faire l'objet de chapitres spécifiques dans la politique de sécurité. En outre il faut encourager et inciter les employés à créer des méthodes de définition de mot de passe robustes. Une méthode très simple mais autant efficace faisant appel à la mnémotechnique est généralement utilisée. Il s'agit de traduire des phrases en mots de passe, en utilisant les premières lettres de chaque mot pour constituer le mot de passe. L'on pourrait inclure des chiffres, caractère spéciaux et lettres majuscules, afin de d'augmenter le niveau de complexité du mot de passe, comme dans l'exemple qui suit.

Phrase : Je suis le père de deux enfants nommés Yves et Marie-claire

Traduction en mot de passe : JslPd2EnY&M-C

J (je) **s** (suis) **l** (le) **P** (père) **d** (de) **2** (deux) **E** (enfants) **n** (nommés) **Y** (yves) & (et) **M-C** (Marie-Claire).

Bien évidemment, il existe de nombreuses techniques de création de mots de passe forts ; qu'il faut mettre en œuvre, afin d'assurer un niveau de force suffisant des mots de passe des employés de l'entreprise. L'utilisation de mots de passe construits en combinant des mots tirés de nos patois peut s'avérer être une stratégie efficace.

De plus, il est préférable d'utiliser des mots de passe différents pour chaque compte (messagerie, bancaire, etc.) et de changer régulièrement les mots de passe (chaque deux mois de préférence).
De nombreux outils en ligne permettent de tester la force de son mot de passe.
https://www.microsoft.com/fr-fr/security/password-checker.aspx
http://www.microsoft.com/canada/fr/athome/security/privacy/password_checker.mspx
http://www.passwordmeter.com

3. Installation d'un antivirus, un anti-troyen, un pare-feu

Chaque ordinateur doit disposer d'un antivirus et d'un anti-troyen puissants et toujours actualisés (application de patches), ainsi que d'un pare-feu correctement configuré par le service informatique. Une mise à jour sera effectuée périodiquement, en fonction des exigences et spécificités de la politique de sécurité.

4. Masquage des propriétés du système

Cette stratégie peut s'appliquer aux personnes qui n'utilisent jamais les connexions à distance, et travaillent toujours sur le même ordinateur fixe, dans le même bureau. Chaque ordinateur sera orné d'une étiquette indiquant le matricule de la machine (ce numéro est celui que les salariés communiqueront au service informatique en cas de défaillance devant être résolue à distance). Les administrateurs auront préalablement interdit l'accès aux propriétés système en mentionnant le nom de l'ordinateur pour éviter toute fuite d'information.
Utiles pour les catégories d'employés qui ont une utilisation assez basique des ordinateurs (secrétaires, juristes, personnels non-techniques, etc.)

5. Désactivation des outils amovibles

Cette stratégie peut s'appliquer si les salariés n'ont pas d'intérêt à utiliser une clé USB, une disquette ou à graver des CD-ROM. Cela dépend de leur définition de fonction et de la nature des activités autorisées au sein de l'entreprise. Cette technique est utilisée dans la plupart des entreprises industrielles et de téléphonie, où les ordinateurs sont tous mis en réseaux et interconnectés entre eux. Ceci permet de limiter voire réduire les risques de contagion virale via les périphériques amovibles (USB, disquettes, etc.) et même de prévenir les risques de fuites d'informations, ou du moins d'en assurer une traçabilité.

6. Etablissement de codes couleur et sensibilité des informations

La hiérarchie et la sensibilité des informations peuvent correspondre à une couleur définie dans un code couleur interne à l'entreprise. Ce système d'autocollants de couleurs est applicable sur les dossiers, sur les pages d'un document physique ou numérique, sur les CD-ROM, définissant ainsi l'importance de la confidentialité du contenu des informations (publiques, sensibles, confidentielles). Aussi, il faut éviter de mettre sur un même support papier ou numérique, des informations de niveau de confidentialité différentes. Les employés auront accès à une catégorie d'information, en fonction de leurs privilèges et des missions qui leur sont assignées

7. Création de messages d'erreur sécurisés

Ne concevez pas de messages d'erreurs automatisés, reproduisant des informations telles qu'un nom d'utilisateur, la version d'un serveur, etc., celles-ci pourraient être utilisées par un attaquant malveillant.

Pour ce faire, configurez l'application de façon à ne pas afficher d'erreurs trop détaillées sur les caractéristiques du matériel utilisé.

Dans le cas où vous souhaitez afficher des messages d'erreur détaillés en vue du débogage, vérifiez préalablement que l'utilisateur est local au serveur Web et créez une gestion des erreurs personnalisée pour les situations sujettes aux erreurs, telles que l'accès aux bases de données.

8. Utilisation sécurisée des cookies

Les cookies sont un moyen simple et utile de conserver des informations propres à l'utilisateur de façon accessible. Toutefois, étant donné que les cookies sont envoyés à l'ordinateur sur lequel s'exécute le navigateur, ils sont vulnérables face à l'usurpation ou à d'autres utilisations malveillantes (session Hi-Jacking, etc.). Au moment de la réalisation d'une transaction sur le web, trois types de menaces pèsent sur les cookies.

i. Les menaces liées au réseau
ii. Les menaces liées aux extrémités du réseau
iii. Les menaces liées à la collecte de cookies

Pour assurer une utilisation sécurisée des cookies, respectez les quelques règles énumérées suivantes :

i. Ne stockez aucune information sensible dans des cookies. *Par exemple*, ne stockez jamais un mot de passe dans un cookie, même de façon temporaire. En règle générale, ne stockez pas d'informations sensibles dans un cookie. Conservez plutôt une référence, dans le cookie, à l'emplacement des informations sur le serveur.
ii. Définissez des délais d'expiration les plus courts possible pour les cookies. Dans la mesure du possible, évitez toujours les cookies permanents.
iii. Envisagez de chiffrer les informations contenues dans les cookies, afin d'offrir une double couche de sécurité à vos cookies.
iv. Envisagez d'affecter *true* aux propriétés Secure et HttpOnly sur vos cookies.

9. Configuration du modem

Les connexions à distance doivent être correctement effectuées et astucieusement cryptées. Les hackers effectuent des scans des modems. Paramétrez votre modem afin qu'il réponde à la cinquième sonnerie.

10. Configuration du fax, du routeur

Le matériel de ce genre est livré avec un mot de passe par défaut ou mot de passe constructeur. La première configuration à réaliser une fois l'appareil installé, est de changer le mot de passe fourni par le fabricant en le remplaçant par un mot de passe complexe, s'appuyant sur les techniques de création de mot de passe robuste. Cette manipulation empêchera les hackers de profiter de ces failles des plus évidentes, mais très souvent laissées par les administrateurs réseaux par ignorance ou négligence.

11. Destruction des informations sensibles ou du matériel contenant des informations sensibles

Les informations sensibles devront être détruites une fois que l'on considérera qu'elles sont devenues inutiles ou obsolètes ou que leur utilisation par d'autres personnes peut s'avérer dangereuse. Les supports physiques seront démagnétisés puis détruits par la suite. Il faut tout de même être très méticuleux dans les processus de destruction des informations sensibles ou de matériel, car dans certains cas, lorsque vous croyez avoir détruit vos données, ces dernières restent dans la Base de registre. En effet, les données de votre disque dur peuvent toujours être récupérées selon certaines méthodes, même quand votre disque dur est brûlé. Des exemples palpables sont disponibles sur le site www.ontrack.fr .

12. Protection des corbeilles à papier et des poubelles

Les poubelles à papier de la majorité des entreprises regorgent d'innombrables informations qui peuvent être subtilisées par un attaquant. Une personne mal attentionnée peut trouver en fouillant dans les poubelles, de nombreuses d'informations de niveau de criticité variable, allant du petit mot entre collègues, au post-it du DAF, jusqu' au précieux mot de passe, etc.

Dans de nombreux cas, les hackers ont fouillé les poubelles d'entreprises, avant d'obtenir des informations stratégiques qu'ils ont par la suite utilisées à leurs fins malveillantes. Vous pourrez utiliser les destructeurs de papier de façon systématique et garder précieusement les corbeilles à papier à l'abri du personnel et du public en général.

13. Les données papier

Les données papier doivent se trouver dans des endroits verrouillés et surveillés par vidéo pour éviter qu'un fouineur malveillant ou indiscret ne puisse accéder à la documentation confidentielle de l'entreprise.

14. Utilisation de systèmes biométriques dans des endroits sensibles

Si l'entreprise conserve des informations sensibles, dont la fuite pourrait compromettre l'avenir de la société, comme la diffusion de secrets commerciaux, de codes source ou de recherches sur de futurs projets avant dépôt d'un brevet, il est indispensable de développer un système de sécurité biométrique. On dispose de trois types d'identification :

i. empreintes digitales ou rétiniennes ;
ii. Reconnaissance faciale ;
iii. Présentation d'un badge infalsifiable.

Certains services de sécurité biométriques ont déjà été l'objet de fraude, d'où la nécessité de combiner tous ces types d'identification ou du moins deux d'entres elles, afin de minimiser les risques d'abus. Bien sûr ceci peut coûter très cher, mais il faut évaluer la criticité des informations que l'on souhaite protéger et faire des investissements en conséquence.

15. Configuration d'un réseau sans fil

De nos jours, les connections s'établissent sans fil et le Wi-Fi remplace le câble. Dans ce cas, il est fortement recommandé d'installer un niveau de cryptage élevé, impliquant l'utilisation d'outils de cryptage de haut niveau, une configuration optimale des matériels de routage. Seul le responsable de la sécurité informatique ou l'administrateur réseau doit connaître ce cryptage. Vous pouvez par exemple :

i. Changer le mot de passe utilisateur de votre routeur Wifi
ii. Changer et cacher le nom de votre réseau (SSID) à la vue des utilisateurs malintentionnés
iii. Désactiver la diffusion du nom SSID de votre réseau
iv. Activer le cryptage de votre réseau, en utilisant de préférence une clef de sécurité de type WPA(Wifi Protect Access)
v. Activer un couplage adresse MAC-adresse IP des ordinateurs qui accèdent à votre réseau

16. Configuration d'un moniteur réseau

Il est impératif que le moniteur réseau, outil de surveillance, soit configuré pour se déclencher régulièrement afin de surveiller les entrées et sorties d'adresses IP, afin de localiser l'adresse IP d'un éventuel intrus essayant d'utiliser la force brute pour pénétrer dans votre système. Il existe également des moniteurs réseau pour les installations sans fil.

17. Installation d'un pare-feu interne et externe

Le système d'informations d'une entreprise doit être protégé derrière un pare-feu externe et disposer de pare-feu internes pour les postes gérant des informations particulièrement sensibles.

18. Les réseaux DMZ (DeMilitarized Zones)

La DMZ (Demilitarized Zone) est un environnement de sous-réseau qui est positionné entre un réseau interne de confiance et un réseau externe non sécurisé. Il s'agit en quelques sortes d'une zone franche de transition entre deux environnements de réseau. En outre, les DMZ constituent la forme la plus courante d'implémentation de pare-feux. Dans le cas d'un tel réseau, deux pare-feux au moins sont necessaires. Par exemple, le serveur VPN est combiné avec le pare-feu principal, tandis que les autres serveurs accessibles de l'extérieur sont positionnés aussi sur la DMZ externe.

Les réseaux DMZ sont ainsi utilisés comme relais de protection pour les serveurs et ressources qui nécessitent d'être accessibles de l'intérieur ou de l'extérieur mais qui ne doivent pas être positionnés dans des réseaux protégés internes. Les serveurs installés dans la partie externe de la DMZ permettent de fournir des services au réseau externe, tout en protégeant le réseau interne contre des intrusions possibles.

19. Réseaux privés virtuels d'entreprise ou Virtual Private Networks (VPN)

La connexion à distance sur un réseau interne d'une PME impose d'utiliser un réseau privé virtuel d'entreprise ou VPN. L'utilisation d'un tel réseau virtuel permet de chiffrer le trafic réseau sensible et requiert une authentification forte, offrant ainsi un accès à distance sécurisé.

En somme, le VPN garantit les trois exigences fondamentales de la sécurité informatique, à savoir :

- ***Intégrité*** : les données reçues par le site principal sont identiques à celles envoyées par le site externe ou le poste nomade,
- ***Confidentialité*** : la propriété privée des données est complètement assurée,
- ***Authentification*** : le récepteur des données sur le site de l'entreprise doit être sûr que les données ont bien été émises par le bon utilisateur. Mise en œuvre de liaisons sécurisées.

Précautions d'utilisation de la fonctionnalité du VPN et les bonnes pratiques

- Le périmètre de sécurité de l'entreprise est étendu avec des environnements (sites ou entreprises) distants qui devront avoir au moins le même niveau ou les mêmes règles de sécurité que le site principal. Le serveur VPN devra être paramétré pour traiter le chiffrement du trafic. Il pourra exister aussi des problèmes d'adressage et des conflits d'adresses possibles, si les deux sites utilisent des parties du même espace d'adressage.
- Avant d'implémenter un réseau virtuel d'entreprise de type VPN, les administrateurs du système doivent évaluer la compatibilité avec le réseau existant. Les directives de sécurité générales proposent les conseils suivants à destination des entreprises utilisant cette fonctionnalité :
- Le principe d'authentification doit utiliser soit un système de mot de passe comme un dispositif à jeton ou un couple de clé publique/privée avec un système identification/mot de passe complexe.
- La déconnexion automatique du réseau d'entreprise doit se produire après une période d'inactivité (à définir). Cette protection impose à l'utilisateur de se reconnecter à l'échéance de cette période.
- Limiter le temps de connexion au VPN, pour éviter d'être surveiller.
- Ne pas permettre une double connexion à partir du même poste nomade.
- Avoir un inventaire de tous les postes externes au site susceptibles de se connecter au site central via le VPN.
- Tous ces équipements doivent être configurés pour être conformes à la politique de la sécurité de l'entreprise, contrôlés fréquemment. Ils doivent

être protégés impérativement contre des logiciels malveillants (antivirus…) avec les signatures les plus récentes.

- Les personnels ayant les possibilités et les privilèges de connexion VPN doivent vérifier que leur compte n'est pas utilisé par des utilisateurs non autorisés.
- L'installation et la maintenance de pare-feu personnels (matériel ou logiciel) du côté utilisateur doivent être requises.

Top 10 des meilleurs logiciels de VPN :

1. ***CyberGhost*** *: Un trafic illimité dans sa version gratuite, mais avec une bande passante faible. Disponible en Français.*
2. ***Security Kiss*** *: Un des VPN les plus populaires. Pour un accès à des serveurs plus rapides, il existe plusieurs offres payantes mais raisonnables. Disponible en Français.*
3. ***Freedom IP*** *: Un VPN totalement gratuit et communautaire. Disponible en Français.*
4. ***Arethusa*** *: Organisation à but non lucratif. Surf web uniquement possible.*
5. ***proXPN*** *: Vitesse limitée à 100KB/s.*
6. ***VPNBOOK*** *: 100% gratuit, mais en anglais.*
7. ***PD-Proxy*** *: Une version premium débride cette version gratuite.*
8. ***Private Tunnel*** *: Limité à 100 Mo.*
9. ***LogMeIn*** *: Gratuit pour les usages non-commerciaux.*
10. ***the Free VPN*** *: Aucune restriction, mais page publicitaire qui s'ouvre sur chaque page.*

20. Les privilèges des utilisateurs

Les privilèges sont accordés au cas par cas et dépendent de nombreux facteurs. Aussi, la demande d'accès du niveau hiérarchique doit être la plus précise possible, afin d'indiquer à l'administrateur les accès à donner ou à interdire, les lecteurs ou dossiers auxquels le salarié devra avoir accès en fonction des tâches qui lui incombent.

21. Formation des employés

Dès leur arrivée dans l'entreprise, les employés (salariés, intérimaires, stagiaires…) doivent prendre connaissance des règles et procédures qui régissent l'entreprise et les suivre à la lettre. Cela évitera de les transformer en proies faciles pour un manipulateur susceptible de se faire passer pour un supérieur hiérarchique, afin d'obtenir des informations sensibles (ingénierie sociale).

D'autre part, le personnel susceptible de travailler à distance doit être formé en matière de cryptage (cryptage des courriers électroniques, cryptage des en-têtes, des fichiers, des dossiers, envoi de fax de façon cryptée, etc.).

Les salariés qui utilisent n'importe quel équipement informatique doivent signer une clause de confidentialité, les soumettant au secret professionnel.

Le règlement concernant l'informatique y est spécifié et stipule qu'il est interdit de révéler le type d'équipement sur lequel le salarié travaille, de révéler son mot de passe ou les programmes exécutés (sans autorisation de son supérieur hiérarchique), les extensions des lignes internes, etc. L'utilisation des économiseurs d'écran, antivirus, anti-troyens, pare-feu, disquettes, clés USB ou de n'importe quel système de stockage de données amovible doit être vérifiée avant l'exécution de son contenu. L'excès de confiance est à éviter, surtout avec le personnel de passage dans l'entreprise.

22. Le personnel et les appels téléphoniques

Avant qu'une personne ne soit prête à recevoir des appels provenant de l'extérieur, avant qu'elle ne soit en relation directe avec les clients, elle doit être informée qu'elle ne doit à aucun moment divulguer de données personnelles, quelles qu'elles soient, ni les règles et procédures internes, ni le numéro de l'extension des lignes téléphoniques, ni bien sûr aucun mot de passe.

23. La ligne téléphonique

Les numéros de lignes directes ne doivent pas être communiqués, ni les adresses email du personnel interne. Il doit exister un numéro d'appel unique, puis les appels sont transmis aux intéressés.
Pareil pour les e-mails : d'abord une adresse générale est communiquée, puis la transmission des emails aux intéressés est effectuée par un personnel bien formé aux stratégies de sécurité.

24. Serveur téléphonique

Protéger votre serveur téléphonique derrière un pare-feu très puissant. De plus, tous les mots de passe du fabricant doivent être changés au moment de sa mise en service.

25. Les lignes téléphoniques avec différentes sonneries

Cette méthode permet de savoir s'il s'agit d'un appel interne ou externe. Les téléphones publics de l'entreprise doivent également être identifiables.

26. Le traçage d'appel

Votre fournisseur d'accès téléphonique peut vous permettre de suivre la trace des appels émis et reçus, afin de pouvoir identifier les appels suspects et de créer un groupe spécifique gérant les données de ce genre d'incidents.

27. Politique de recrutement

Faire attention à ceux qu'on embauche ou avec qui l'on traite en effectuant une enquête poussée pour les préposés à des postes sensibles de sécurité. Il est de

coutume pour de nombreuses entreprises d'envoyer des taupes en mission d'infiltration dans les entreprises concurrentes. En effet, la concurrence se faisant grande, l'expertise rare, les entreprises ont tendance à courir parfois aveuglément derrière les perles rares de l'industrie de la sécurité.

28. Maintenance de site web

Plusieurs entreprises laissent leurs sites en ligne lorsqu'ils sont en développement. Si le niveau de sécurité est faible, le pirate pourra trouver un exploit pour profiter des vulnérabilités des pages web. Les sites en cours de développement ne doivent pas avoir de liaisons avec le réseau, afin d'éviter des attaques de l'extérieur ou de l'intérieur. En Côte d'Ivoire, le CI-CERT à travers son système de surveillance de site web (SysWeb) est un partenaire de premier choix, en la matière.

29. Configuration de serveur SQL

Ne pas installer le serveur SQL sur le serveur IIS, car les pirates peuvent utiliser des failles pour envoyer des commandes par le biais du Web. Si vous travaillez avec un serveur SQL, il convient d'éliminer les utilitaires inutiles et utiliser des mots de passe autres que les mots de passe par défaut, afin d'éviter qu'un pirate ne s'introduise dans votre système à distance au moyen de l'invite de commandes, « **xp_cmdshel"l** » par exemple.
Désactiver le protocole ICMP, et/ou utiliser des détecteurs d'intrus de marques très connues.

30. Ports de serveurs

Désactiver les ports inutilisés dans le commutateur et s'assurer que les autres soit suffisamment sécurisés afin de pouvoir empêcher des attaques d'empoisonnement ARP, d'inondation d'adresses MAC ou les usurpations d'adresses.

Installer des détecteurs d'intrus IPS dans le réseau afin d'être averti qu'une attaque tente d'être menée. On peut également utiliser les sniffers qui capturent les données du réseau.

31. Patches et mises à jour

S'informer régulièrement sur les nouvelles actions correctives disponibles relatives aux patches, en mettant un accent particulier sur la veille technologique en matière de sécurité informatique. Il faut également s'assurer de la disponibilité de mises à jour régulières, avant d'adopter un logiciel censé abriter ou protéger des données sensibles pour son entreprise. Dans la majorité des cas, les constructeurs de logiciels propriétaires, assurent un suivi méticuleux de la sécurité des produits qu'ils commercialisent, à travers la diffusion régulière de mises à jour de sécurité. De l'autre coté, les communautés de logiciels libres sont également une force vive pour les adeptes du libre.

32. Restriction d'utilisation du matériel informatique professionnel

Mettre des restrictions en place afin que les utilisateurs ne puissent pas installer des exécutables téléchargés sur Internet. Ces mesures permettent de limiter les risques d'installations de logiciels malveillants sur le réseau de l'entreprise.
Mais avec le développement du BYOD (Bring your Own Device), la tâche se complexifie un peu plus. En effet, il faut arriver à concilier les intérêts des employés et ceux de l'employeur en mettent en place des mécanismes adaptés à la culture, aux objectifs et moyens de l'entreprise.
Garder les informations sensibles, par exemple la configuration du DNS ou les listes de partenaires commerciaux privées et sécrètes et ne jamais les publier sur une page publique.

Quelques règles de protection des appareils personnels dans le cas d'un BYOD :

i. Appliquer les mots de passe robustes sur les périphériques personnels (soumettre les équipements personnels aux mêmes règles que l'ensemble du matériel informatique, tel que définit dans la PSSI)
ii. Chiffrer intégralement les disques durs, les périphériques amovibles et les données stockées dans le Cloud
iii. Activer un système de gestion des périphériques, afin de supprimer les données contenues sur les périphériques perdus ou volés
iv. Contrôler les applications installées
v. Utiliser un tunnel VPN chiffré et une authentification à deux facteurs pour les applications critiques de l'entreprise

33. Gestion des intrusions

Créer des filtres pour interdire les adresses IP et sites suspects, émettant un nombre de requêtes supérieur à la normale (tenant compte des activités et du niveau de privilège de l'utilisateur). Ce type d'outil, pouvant être associé à d'autres outils de gestion des vulnérabilités, permet de scanner chaque serveur en le testant à partir d'un catalogue d'évènements. L'un des plus connus s'appelle **Nessus**. C'est un outil gratuit de recherche de vulnérabilités pour les réseaux, disponible à l'adresse : www.nessus.org .

Par précaution, les administrateurs du réseau doivent être avertis que cet outil, s'il est configuré efficacement, peut générer des journaux d'évènements volumineux qui doivent être analysés attentivement. Il est donc recommandé de positionner l'IDS dans tout endroit où le trafic réseau venant de l'extérieur est utilisé avec des VPNs. Il existe des outils plus performants qui bénéficient généralement d'une mise à jour continue de la base de données des attaques : celle-ci regroupe toutes les signatures des attaques référencées. Deux "méthodes" sont utilisées selon les outils : une surveillance du système et un signalement de toute action suspecte, ou la comparaison de toutes les requêtes au signalement des attaques les plus connues.

34. Gestion des protocoles de communication

Réduire la bande passante et limiter le débit de trafic pour certains protocoles de communication (création des piles personnalisées).

35. Utilisation de « honey pot »

Créer des pages fictives afin d'envoyer les connexions suspectes dans un trou noir. Créer des « **honey pot** » ou « pots de miel » permet d'attirer les pirates vers de fausses cibles rendues volontairement vulnérables, afin d'étudier les techniques d'attaques, identifier et pister les attaquants.

Les sites web doivent constamment effectuer des sauvegardes et changer les mots de passe des gens qui se connectent fréquemment. L'administrateur devra donner aux partenaires ou aux utilisateurs qui travaillent à distance des mots de passe temporaires que chaque utilisateur modifiera très régulièrement.

36. Adresses e-mails à éviter

Cette précaution concerne plus les risques de spamming que de hacking. En effet, les adresses e-mails qui ont les préfixes les plus courants sont les plus faciles à spammées automatiquement grâce à des outils gratuits disponibles sur le net (car ils ont plus de chances d'exister). Il serait judicieux d'éviter de créer des adresses avec les noms suivants: webmaster@, admin@ contact@, email@, mail@, info@, sales@, support@, root@, www@, abuse@ news@,etc.

Une autre technique très astucieuse consiste à créer des images sous un format reconnu (jpeg, jpg, etc.), qui contiendra l'ensemble des informations de contacts de l'entreprise. Cette technique permet d'éviter l'indexation par les robots des moteurs de recherche et autre logiciels de récupération d'adresse électronique sur Internet.

37. Cryptage de votre adresse e-mail

Lorsque vous affichez une adresse e-mail sur votre site web, vous avez 2 solutions:

1) Créez un fichier image (gif, png, jpeg) avec votre adresse écrite dessus. Ce n'est pas du texte et les robots spammeurs ne le verront pas. Ils ne pourront donc pas vous envoyer automatiquement du spam
2) Utilisez des solutions de cryptage de vos e-mails (*PGP* par exemple)
3) Cryptez votre adresse e-mail avec du JavaScript. De nombreux sites comme celui-ci : www.aspirine.org, proposent des services en ligne de ce genre. Pour les entreprises dotées de plus de moyens, d'autres méthodes encore plus poussées existent pour faire crypter les e-mails

CONCLUSION

La sécurité informatique, comme nous l'avons examiné, relève de la conjugaison de plusieurs efforts tant juridiques, technologiques que managériaux. Le système d'information est de nos jours, au cœur de toutes les entreprises modernes. Les nombreux avantages et les opportunités immenses qu'offre le réseau des réseaux, font d'Internet un enjeu économique capital. Les nombreux modèles d'entreprises développées en utilisant la puissance d'Internet (Dell, Facebook, etc.), montrent à quel point les systèmes d'Informations ont acquis une place de premier choix dans la vie et le développement des entreprises. La sécurité par définition, est une réponse à un état d'insécurité, permettant d'installer la confiance. Si de nombreuses entreprises et organisations ont consentis des efforts énormes dans la course vers les technologies pour assurer la sécurité de leurs SI, force est de constater que les réponses proposées restent bien souvent inopérantes ou insatisfaisantes. En effet, les technologies de l'information et de la communication sont très évolutives et la criminalité informatique suit cette dynamique.

Faire reposer la sécurité sur les seuls « armes technico-technologiques », est donc similaire à traiter les symptômes du mal, sans en atteindre la racine. Cette démarche s'inscrit inévitablement dans le court terme, en proposant des solutions superficielles amenées à être dépassées, en même temps que les technologies.

La criminologie présente la criminalité comme le résultat d'une conjugaison de facteurs multiples, qu'il convient de d'analyser au cas par cas. D'un point de vue criminologique, le crime et tous les actes de déviance doivent être analysés comme des composantes fondamentales de la société. Selon E. Durkheim : « […] le crime est un fait normal ». Le crime est normal, parce qu'une société qui en serait exempte est tout à fait impossible ; telle est la première évidence paradoxale que fait surgir la réflexion sociologique. Ceci dit, la conception de la sécurité informatique infaillible et basée sur des mesures technologiques de pointe relève de l'utopie.

En somme, il apparait plus que nécessaire pour les entreprises, de concevoir la sécurité informatique selon une approche globale et multidimensionnelle. En effet, faire de la sécurité informatique ne relève pas exclusivement de la compétence des ingénieurs et techniciens informatiques. En plus de l'adoption d'outils technologiques, il est plus que jamais nécessaire d'intégrer :

- Les aspects organisationnels (création de directions, départements, service et organe de sécurité des systèmes d'information, de management des risques)
- Les aspects de management (développement d'une culture de sécurité, gestion des ressources humaines, formation et sensibilisation)
- Les aspects juridiques (prise en compte de la gestion des risques informatique, dans la rédaction des contrats, règlements intérieurs, charte, etc.)
- La prise en compte de la relative "fragilité" de l'être humain (stress au travail, erreurs, santé physique et émotionnelle, traitement social et salarial, etc.)

De plus, les utilisateurs des technologies devront intégrer le fait que les technologies, aussi avancées soient-elles, demeurent des œuvres humaines, donc imparfaites. Car c'est là, la véritable clé du problème. En adoptant une position de réserve à l'égard des TIC, l'Homme se remet au cœur du processus de développement, afin que « l'humain » demeure le maître de la « machine ».

Si les pays dits développés consacrent des parts de budgets colossales à la recherche scientifique en générale et aux TIC en particulier, c'est dire l'importance de cette discipline dans le développement des nations.

A l'heure où le monde s'achemine résolument vers les autoroutes de l'information à travers l'apparition de IP-v6, il apparait plus que nécessaire pour nos Etats et jeunes entreprises Africaines de se doter d'infrastructures, ressources technologiques et de connaissances, afin de participer pleinement au développement de la société numérique mondiale. Car s'il est vrai que l'Afrique, comme dans bien des domaines est un super-consommateur des produits provenant du Nord, nul ne saurait nier le potentiel énorme dont elle regorge et le rôle prépondérant qu'elle pourrait jouer dans la société du numérique.

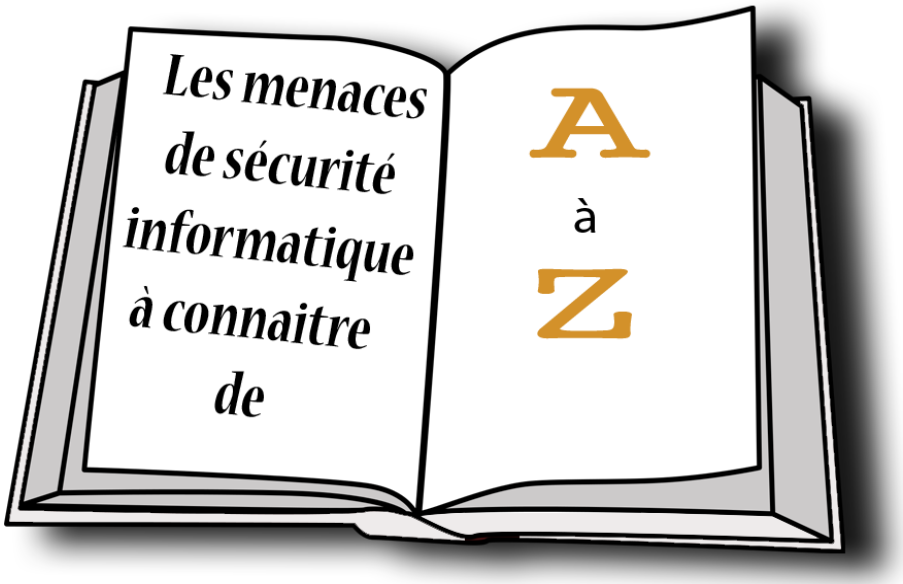
Les plus grands experts en sécurité informatique, conviennent qu'aucune règle ou mesure de sécurité informatique n'est infaillible, d'où l'intégration de la notion de défense en profondeur dans la conception de la sécurité informatique. La sécurité informatique mérite d'être appréhendée dans son entièreté, afin de définir des stratégies efficaces et adaptées aux objectifs de l'entreprise et même des gouvernements, car de plus en plus l'Etat apparait comme un actionnaire des entreprises du privé.

Loin de se résumer à une course effrénée aux outils technologiques, la sécurité devrait plutôt être perçue comme un véritable concept stratégique, découlant d'une culture intégrée au sein de l'entreprise et même hors de celle-ci. En effet, la démarche sécurité est un projet d'entreprise dont la réalisation engage chaque membre de l'entreprise en tant qu'acteur principal. La sécurité est dorénavant appréhendée et traitée comme un processus continu.

Par ailleurs, intégrer la sécurité en tant que « processus » met en lumière la dimension managériale et stratégique de la **sécurité informatique**. L'objectif clé de cette démarche étant d'optimiser et rationnaliser des investissements, tout en assurant la pérennité et l'efficacité des solutions de sécurité dans le temps.

THESAURUS DE LA

SECURITE INFORMATIQUE



A

Adware (publiciel):

« Advertising-supported software » ou publiciel

Logiciel généralement gratuit qui diffuse automatiquement de la publicité sur votre ordinateur, lorsque vous l'utilisez. Les publiciels ne sont pas nécessairement nuisibles, car ils peuvent aider au développement de programmes gratuits à travers les fonds récoltés par la publicité diffusée. Mais ils peuvent également s'avérer nocifs et dérangeant, par exemple quand il s diffusent de la publicité intempestive et dérangent ainsi le confort de navigation sur Internet de l'utilisateur.

APT (Advanced Persistent Threats):

Les APT ou Attaques persistantes avancées sont des attaques de type très ciblé et persistante. Dans ce genre d'attaque, le pirate s'inscrit dans la durée en se maintenant de façon très subtile durant de longs moments dans le système, afin de collecter des données sensibles. Ces attaques sont souvent le fruit d'une attaque longue et minutieuse contre une cible spécifiquement choisie.

Autorun worm *(Vers autorun):*

Logiciels malveillants qui s'exécutent automatiquement en utilisant la propriété « *autorun* » de Windows. Une fois le périphérique infecté est connecté sur l'ordinateur, le programme malveillant s'exécute automatiquement.

B

Backdoor

Logiciel malveillant qui permet de prendre le contrôle de la machine d'un utilisateur via Internet, sans aucune permission. C'est une sorte de programme qui crée à l'insu du propriétaire de l'ordinateur un accès totale à son système. Une fois le backdoor installé, il s'incorpore dans le fonctionnement normal de l'ordinateur et est toujours exploitable même après le redémarrage de l'ordinateur. L'attaquant qui installe un backdoor sur la machine d'une victime dispose ainsi d'un accès large à l'ensemble des activités qui y sont menées.

Boot sector malware

(Logiciel malveillant affectant le secteur de démarrage)

Logiciel malveillant modifie le *boot sector* ou secteur de démarrage, portion de disque utilisée par le système d'exploitation pour démarrer. Il modifie le secteur légitime et ordonne au système d'exploitation de démarrer à partir d'un secteur infecté contenue dans le programme malveillant. Une fois que l'ordinateur redémarre, le programme malveillant est lancé et s'exécute donc sur l'ordinateur.

BOTNET

Réseau d'ordinateurs contrôlés à distance par un pirate informatique. L'ensemble des machines constituant le réseau sont contrôlé à l'insu de leurs propriétaires en utilisant différentes techniques de hacking. Les réseaux de botnet sont particulièrement dangereux, car leur degré de nuisance peut être extrêmement grand, plus le nombre de machines contrôlés (zombies) est grand. Le pirate contrôlant le réseau appelé le botmaster, peut lancer des attaques massives en utilisant ces machines contrôlées, afin de masquer la véritable origine de l'attaque. Pour l'entreprise les risques sont énormes, dans le cas des machines du parc informatique d'une entreprise sont impliqués dans une attaque informatique contre un système d'informations.

Bug ou bogue:

Dysfonctionnement d'un programme ou d'un matériel survenant suite à une erreur involontaire de programmation (conception) ou de construction. La gravité peut varier et avoir un impact plus ou moins sur l'intégrité et le fonctionnement du logiciel ou du matériel informatique.

Browser hijacker:

ou détourneur de navigateur

Logiciel malveillant qui modifie sans votre consentement les réglages de votre navigateur web. Il est capable de changer la page d'accueil, la barre de recherche, etc. Cette attaque peut être utilisée par un pirate pour booster les revenus générés par un site web, en modifiant le comportement de votre navigateur.

Brute force :

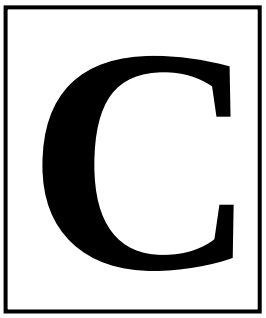
ou attaque par force brute

Technique qui consiste à utiliser un très grand nombre de mots de passe, afin de gagner un accès non autorisé à un système d'information ou un compte protégé par mot de passe. L'attaquant utilise des programmes informatiques, qui à l'aide d'un algorithme spécialement conçu, vont tenter un nombre très grand de

combinaisons, afin de trouver un mot de passe.

Buffer overflow :

Un ***buffer overflow*** se produit lorsqu'un programme stocke les données excédentaires en écrasant les autres parties de la mémoire de l'ordinateur, provoquant des erreurs ou des plantages du système. Les attaques de type buffer overflow exploitent une vulnérabilité d'un logiciel, en lui envoyant un volume de données plus grand que celui auquel il s'attendait. Le programme se voit contraint de traiter un volume de donnée plus grand, que l'espace mémoire prévue à ces fins et efface donc les espace mémoire utilisés par le système d'exploitation.



Captcha

Forme de test d'authentification utilisé pour déterminer si un programme ou un service en ligne vient d'une nature humaine ou de l'utilisation d'une machine. La principale forme de Captcha est générée avec des images de manière aléatoire, qui contient des codes à saisir à l'identique dans une boite de dialogue. Une machine ne peut pas décoder des lettres et des chiffres intentionnellement déformés. Cela permet de s'assurer que (par

exemple) un programme ne peut pas être désactivé par un autre programme ou par Bot.

Cheval de Troie

ou Trojan Horse

Logiciel d'apparence inoffensive mais qui cache sous sa face apparent un programme malveillant, qui une fois entré dans le système libère sa charge nocive (logiciel malveillant). Le cheval de Troie se présente comme un programme ne réalisant qu'une simple action inoffensive, mais contient d'autres fonctions malicieuses cachées qui s'activent une fois le logiciel installé sur l'ordinateur de la victime. De nombreux programmes gratuits contiennent des chevaux de Troie de nos jours.

Crack

Outil de Hacking utilisé pour décoder des mots de passe encryptés. Les administrateurs utilisent aussi Crack pour évaluer la faiblesse des mots de passe des utilisateurs inexpérimentés dans le but d'augmenter la sécurité du système.

Cookies :

ou témoins de connexion

Fichiers qui sont placés sur votre ordinateur, afin de permettre aux sites web que vous consultez de se souvenir de certains détails de navigation. Ils sont très utiles, afin d'accroître les performances des sites web et assurer un confort de navigation aux utilisateurs.

D

DoS (Denial of Service):

Attaque informatique dont le but est de submerger de requêtes une périphérique (serveur, logiciel, etc.), afin de rendre inaccessible des services aux utilisateurs. Les sites web sont les plus visés par ce type d'attaque au cours des lesquelles aucune donnée n'est volée, mais l'objectifs est de rendre les services inaccessibles. Le ***DDOS*** ou Distributed denial of service est une variation de l'attaque DoS, dans laquelle les attaques sont envoyées à partir de plusieurs machines contrôlées à l'insu de leurs propriétaires (botnet, zombie) par le pirate.

DNS Hijacking

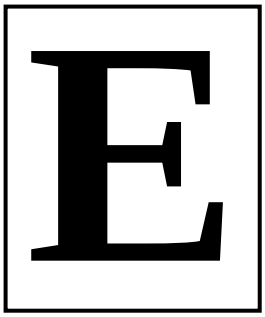
(Détournement de DNS):

Attaque qui consiste à détourner, afin d'utiliser sans le consentement du propriétaire un DNS. Un DNS ou (Domain Name server) est un dispositif qui permet à l'ordinateur de transcrire les noms de sites web ou de blogs (ex : www.cybercrimactu.wordpress.com) en adresses IP, afin que les machines puissent communiquer entre elles. Cette attaque peut permettre de modifier les paramètres d'un ordinateur afin qu'il ignore un DNS légitime et qu'il reconnaisse comme légitime un DNS contrôlé par un pirate malveillant. Ainsi le pirate peut rediriger les informations qu'un utilisateur souhaite envoyer à un serveur légitime vers son propre

serveur, afin de récupérer les informations sensibles telles que mot de passe, login, numéro de carte bancaire, etc.

Drive by download:

Attaque qui consiste à compromettre un site web légitime avec un malware, afin d'infecter les ordinateurs des utilisateurs qui viendront se connecter au site web compromis. Les pirates injectent du code malveillant dans les pages d'un site web légitime et généralement très visité. Une fois que l'utilisateur se connecte à se site web compromis, le code malveillant exploitent des vulnérabilités présentent dans le navigateur web et s'installe sur la machine de sa victime. Ainsi, le pirate peut prendre le contrôle de la machine et commettre de nombreuses infractions (vol et modification de données, botnet, etc.).



Exploit :

Dans le langage de la sécurité informatique, un exploit désigne le moyen utilisé pour tirer profit d'une vulnérabilité. Il peut s'agir d'un logiciel ou d'un code malveillant qui est utilisé pour exploiter la faille de sécurité détectée. L'exploit n'a de valeur que tant que la vulnérabilité pour laquelle il est conçu n'est pas corrigée.

H

Hacker ou (fouineur)

Personne dotée de compétence en programmation et aimant explorer les détails du fonctionnement des systèmes informatiques. La finalité de cette quête de compréhension du fonctionnement des systèmes informatiques définit, la qualification du hacker. Ainsi il existe des *bons* hackers (*White hat hackers qui sont des professionnels de sécurité, généralement employés dans des organismes officiels pour assurer la sécurité des SI*), des *mauvais* hackers (*Black hat hackers qui utilisent leur connaissances dans le but de commettre des activités illicites : vols de données, DoS, etc.*). Il existe également une catégorie de hackers dit hacker gris (Grey hat hacker), ils sont généralement des white hacker mais peuvent virer au black hat hacking, à la faveur de circonstances diverses (idéologiques, politiques, etc.)

Hacking :

Art pratiqué par le hacker

Hacktivisme :

Forme d'utilisation du hacking à des fins purement idéologiques (politiques, religieuses, etc.). Les hacktivistes s'attaquent à des organisations, corporations, entités dont l'activité est antagoniste à la leur.

Hoax (canular)

Fausses rumeurs véhiculées sur Internet. De telles rumeurs peuvent conduire des utilisateurs à utiliser des

types spécifiques de matériel ou logiciel au détriment de d'autres. Dans le cas d'entreprises concurrentes, cette technique peut avoir des effets désastreux.

Honeypot

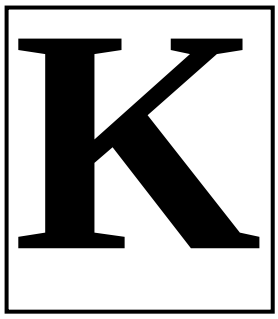
ou pot de miel

Sorte de trappe crée par des spécialistes de la sécurité, afin de conduire des pirates à attaquer une cible délibérément rendue vulnérable. Cette technique est utilisée dans le but d'étudier la stratégie utilisée par les attaquants, afin d'en maitriser les subtilités et prendre des mesures correctives.

HTTPS

(Hypertext Transfert Protocol Secure)

Protocole de communication client-serveur c'est-à-dire entre les ressources manipulées par l'utilisateur (navigateur) et les ressources utilisées pour le fonctionnement des sites web (serveurs). Le protocole de base est le http et le HTTPS désigne une version sécurisée de cet protocole, en utilisant les protocoles de sécurité SSL ou TLS. Le protocole **https** est utilisé dans le cadre d'échanges sécurisés sur des sites web, notamment quand il faut saisi un mot de passe, un numéro de carte de crédit, etc.



Keylogging : Le keylogging ou enregistrement de frappes est une technique qui permet à l'insu d'un utilisateur, d'enregistrer toutes les frappes qui sont effectuées sur le clavier d'un ordinateur ou de tout

autre périphérique tactile. Ainsi le pirate peut récupérer des informations sensibles (login, mot de passe, etc.) saisies par l'utilisateur d'un ordinateur sur lequel est installé un keylogger.

Les keyloggers sont des programmes informatiques ou périphériques amovibles, qui permettent de réaliser le keylogging.

L

Lettre à la chaine :

E-mail dont le contenu vous incite à faire suivre et partager à un plus grand nombre de personnes. Cette technique peut être utilisée pour véhiculer des malware ou encore récupérer un grand d'adresse électronique de collègues, proches, etc. *Ex* : Pétitions, messages de soutien, etc.

Logic Bomb :

Aussi connu sous le nom de Fork Bomb, il s'agit d'un programme résidant sur un système informatique qui une fois lancé, recherche une condition ou un état particulier du système pour exécuter une action illicite une fois cette condition trouvée. Il permet de réaliser une action précise si une condition définie par son auteur est vérifiée. *Ex : éteindre l'ordinateur si la webcam est allumée*

M

Malware

ou logiciel malveillant

Terme générique utilisé pour désigné tout les programmes malveillants, tels que Virus, Vers, Chevaux de Troie, etc. De nombreuses variations d'utilisation des malwares existent, à savoir :

- E-mail Malware (en utilisant un e-mail pour véhiculer le malware)
- Document Malware (en camouflant le malware dans un document PDF, Word, Excel, etc.)
- Mobile Phone Malware (en utilisant le téléphone mobile comme vecteur de propagation)
- Etc.

Mail-bombing:

Consiste en l'envoi massif de messages électronique identique vers le même destinataire à l'effet de saturer le serveur de mails, saturer la bande passante du serveur et du ou des destinataires ou de rendre impossible aux destinataires de continuer à utiliser l'adresse électronique. La trop grande quantité de e-mail envoyé simultanément rends inutilisable les services de messagerie.

P

Patches

Les patches sont des programmes informatiques qui sont utilisés pour corriger des failles ou vulnérabilités découvertes dans un logiciel informatique. Ces correctifs sont généralement crées suite à la découverte d'une faille ou bug dans le affectant le fonctionnement ou la sécurité d'un logiciel informatique. Les patches sont des applicatifs de sécurité qui viennent combler des insuffisances de sécurité qui se révèlent à l'usure d'un logiciel (OS, antivirus, etc.).Tous les grands fabricants de solutions informatiques proposent des patches pour leurs différents logiciels.

Phishing

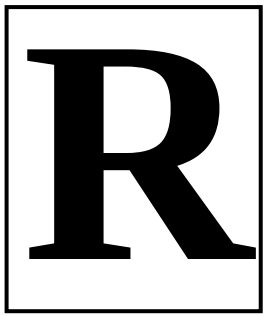
Le phishing est une technique d'arnaque qui consiste à récolter illicitement des données sensibles (mot de passe, login, numéro de carte de crédit, etc.) de personnes tierces, en utilisant la tromperie. L'attaquant procède en envoyant de faux liens cliquables ou un formulaire à remplir, en usurpant l'identité d'un requérant légitime et reconnu (banque, yahoo, facebook, etc.). Dans la majorité des cas, il s'agit d'un e-mail envoyé au nom d'organisme reconnu, vous incitant communiquer des données sensibles via un formulaire ou via un lien qui vous redirige sur un faux site copie presque conforme au site original.

Pour en savoir plus sur le phishing

Phreaking

Forme de « hacking » qui consiste à pirater le réseau téléphonique, afin d'en tirer un avantage quelconque. Il s'agit dans la plupart des cas de réussir à téléphoner gratuitement, en utilisant des techniques diverses telles que :

- Le Blue-Boxing : Les phreakers téléphonent a des numéros verts gratuits, à qui ils envoient un son de 2600 MHz (équivalent au signal qui indique qu'un appel est terminé) grâce a des logiciels. Ce son envoyé fait croire au central du numéro que l'utilisateur a raccroché, alors qu'il est toujours en ligne. Ensuite ils n'ont qu'à effectuer un Out-Dial qui permet d'appeler a l'extérieur et ils téléphonent où ils veulent gratuitement.
- Les Box: Il s'agit de trafiquer des branchages électriques de son téléphone pour obtenir des fonctions qui vous facilitent la tâche. La plus célèbre des boxes est la Black Box : elle permet à celui qui vous appelle de ne pas payer les communications. Il existe plusieurs types de boxes (beige, gold, etc.).
- Etc.



Ransomware

ou rançongiciel

Programme malveillant qui une fois installé sur votre ordinateur ou sur votre Smartphone, vous empêche d'avoir accès à vos fichiers et autres fonctionnalités de votre système d'exploitation. Ces programmes exigent le paiement des rançons à leur propriétaires via paiement électronique, afin de débloquer l'accès aux fichiers ou autres fonctionnalités de votre OS, d'où le nom de rançongiciel. De façon imagée, il s'git d'un logiciel qui prend en otage votre ordinateur et exige le paiement d'une rançon afin de le *libérer*.

Rootkit

Portion d'un programme informatique qui cache son activité et les processus qu'il exécute sur un ordinateur, afin de rester totalement indétectable. Ce genre de programme malveillant est utilisé pour cacher les activités malveillantes menées par l'attaquant. Un rootkit peut cacher des keyloggers ou des renifleurs de mots de passe, installés sur un ordinateur.

S

Social engineering

ou ingénierie sociale

Technique d'arnaque qui consiste à emmener la victime à réaliser des actions que l'on lui intime de faire, en usant de persuasion, d'audace, de manipulation, etc. Cette technique est généralement utilisée pour obtenir des renseignements sensibles, qui une fois récupérés sont utilisés à des fins malveillantes par l'attaquant. [97]

Sniffer

Outil matériel ou logiciel dont l'objet est de capturer les trames transitant sur le réseau. Ce genre de dispositif est utilisé afin de d'intercepter les informations sensibles qui circulent dans le réseau, sous formes de paquets de données. Il peut s'agir de mots de passe, login, numéros de carte de crédit, courriers électroniques, etc. Lorsque les informations échangées entre les différents segments du réseau (utilisateurs) ne sont cryptées, un attaquant peut aisément intercepter et reconstituer les paquets afin de lire en clair les informations échangées.

Spoofing

ou mimicking ou usurpation

Action malveillante qui consiste à utiliser délibérément et sans autorisation de son propriétaire une ressource informatique en lieu et place de la sienne. C'est le fait pour l'attaquant d'usurper « l'identité » d'un système informatique, afin de se

faire passer pour celui. Comme dans les cas d'usurpation d'identité, l'utilisateur malveillant se fait passer pour une personne qu'elle n'est pas, afin de bénéficier de privilèges et mener des activités favorisées par l'identité usurpée. Un attaquant peut ainsi recevoir des informations destinées à l'adresse légitime qu'il usurpe. L'usurpation ou le spoofing peut prendre plusieurs formes, à savoir :

- *MAC spoofing*: usurpation de l'adresse MAC (medium access control, *identifiant physique utilisé pour attribuer mondialement une adresse unique à une machine*)
- *IP spoofing*: usurpation d'adresse IP (Internet Protocol)
- *DNS spoofing*: usurpation de DNS (Domain Name System, *système qui permet de traduire les noms de domaines en informations tangibles pour la machine, tel que l'adresse IP*)
- *Mail spoofing*: usurpation d'une adresse e-mail, afin d'envoyer des courriels au nom d'une personne tierce de laquelle l'attaquant à usurper l'identité.
- *Caller ID spoofing* : usurpation de l'identité de l'émetteur d'un appel, afin de tromper le récepteur de l'appel sur la vraie identité de l'appelant.

Spam

ou pourriel

Message électronique non sollicité reçu de destinataires que l'on ne connait pas ou de qui l'on n'attend pas un e-mail. D'apparence peu offensive, les spams peuvent rapidement devenir très gênant quand les messages reçus atteignent un grand nombre. En effet, certains outils spécialement conçus pour le spam peuvent envoyer des centaines d'e-mails non désirés à la minute. En plus de l'inconfort que cela peut entrainer pour l'utilisateur les risques d'infections par e-mail malware, phishing sont accrus.

Spear-phishing

Forme particulière de phishing très ciblée. Contrairement au phishing classique, le spear phishing nécessite une personnalisation des appâts (e-mails, liens, formulaires, etc.) envoyés à la victime. En effet, l'attaquant récolte un maximum d'informations sur sa victime, afin de maximiser ses chances de succès.

Spyware ou espiogiciel

Programme malveillant qui est destiné à espionner, épier les habitudes de navigation, etc. de l'utilisateur sur l'ordinateur de qui il est installé. Cette technique est utilisée afin de récolter des informations telles que ; les sites web visités, mots clés saisis, achats effectués sur le web ; afin de dresser un profil de l'utilisateur. Cette technique est majoritairement par les entreprises commerciales, afin d'épier les utilisateurs et proposer des produits adaptés aux habitudes des utlisateurs, conférant un avantage certain dans un contexte concurrentiel.

SQL injection : ou injection SQL[16]

Exploit (technique de hacking) qui s'appuie sur les requêtes envoyées vers les bases de données de logiciels, applications, qui ne contrôlent pas suffisamment les accès vers ces dites bases de données. Cette technique permet d'accéder à l'ensemble des données stockées dans la base de données d'un site, en passant par l'interface du site web. Dans les champs de saisis du site web, l'attaquant saisis des commandes (requêtes SQL) afin d'exécuter des actions non prévues par le concepteur du site. En effet, en lieu et place de ses noms et prénoms, l'attaquant peut saisir une commande qui lui permettra d'extraire les noms et prénoms de l'ensemble des utilisateurs stockées dans la base de données. Les WAF (web application firewall) permettent de diminuer les risques liés à cette attaque en analysant les requêtes SQL envoyées au serveur web via l'interface web.

[16] Structured Query Language ou langage de requêtes structurées. Langage utilisé pour la gestion et l'interaction avec les bases de données

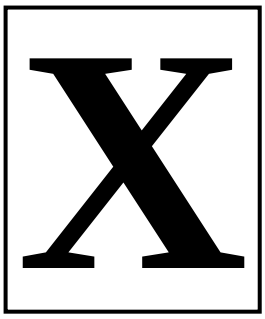
V

Virus

Programmes malveillants extrêmement nuisibles et dont l'action peut avoir des conséquences très graves sur le système infecté, tel que : vol, suppression de données, désactivation de logiciels ou fonctions essentielles d'un système, crash, destruction totale du système, etc. Ces programmes ont la capacité de se rependre d'un ordinateur à un autre, d'un réseau à un autre, en créant des copies d'eux même sans que vous n'en ayez conscience.

Vulnérabilité (Vulnerability) :

Faille, une brèche laissée par malveillance ou maladresse, dans les spécifications, la conception, la réalisation, l'installation ou la configuration d'un système, ou dans la façon de l'utiliser. A la différence d'un bug, une vulnérabilité n'impacte pas le fonctionnement du logiciel ou du matériel ; mais constitue un risque de sécurité qui exploité par une personne malveillante, peut avoir des conséquences extrêmement pour l'utilisateur. Les vulnérabilités sont corrigées par des patches.



XSS (cross-site scripting)

Technique qui consiste à injecter du code malveillant dans des pages web. Ces attaques visent les sites web qui ne contrôlent pas suffisamment le contenu que les utilisateurs du site web sont autorisés à transmettre via les formulaires. Si dans les SQL injections c'est la base de données qui est ciblée, dans les attaques XSS le site web est forcé à exécuter ou afficher le code HTM ou les scripts saisis par les utilisateurs. Ainsi, un utilisateur malveillant peut en injectant du code malicieux dans les pages d'un site vulnérable, déclencher de nombreuses actions, telles que :

- Redirection des utilisateurs qui visitent le site légitime vers un faux site
- Vol de session
- etc.

Z

Zero-Day (attaque 0 day)

Faille de sécurité présente dans un logiciel et qui n'est pas connue du grand public et pas même par l'éditeur dudit logiciel. La faille et les moyens de l'exploiter ne sont connus que par un nombre restreint de personnes, ce qui augmente le potentiel destructeur de l'attaque.

Quand une faille informatique n'est pas publiée, ou connue du grand public, et donc corrigée (patchée) par l'éditeur du logiciel mis en cause, le hacker qui exploite la faille **zero day** bénéficie d'une relative facilité à mener son attaque, étant donné qu'aucune mesure de protection n'est prévue. Il peut par conséquent prendre le contrôle d'un ordinateur, d'un logiciel ou d'un réseau, voire effectuer une attaque par déni de service, sans que la l'utilisateur visé n'ait eu le temps de s'y préparer.

Zombie

Ordinateur contrôlé à l'insu de son propriétaire par un hacker et faisant partie d'un réseau de botnet. Cet ordinateur obéît aux ordres du bot-master (hacker qui contrôle le BOTNET) et peut être utilisé pour lancer des attaques contre d'autres ordinateurs. Pour l'entreprise les conséquences peuvent être énormes tant le plan juridique, que financier.

REFERENCES DOCUMENTAIRES

ilo.org. [En ligne] http://www.ilo.org/dyn/natlex/docs/WEBTEXT/39815/64951/F95CIV01.htm.

legis.ci. [En ligne] http://legis.ci/questionsreponsestravaillicenciementphp.php.

Baptiste, Philippe Jean. *La criminalité Informatique dans l'entreprise: les aspects techniques et légaux de la preuve.*

CI-CERT. [En ligne] http://www.cicert.ci/.

CIGREF. [En ligne] http://www.cigref.fr/.

CLUSIF. [En ligne] http://www.clusif.asso.fr.

—. *Le rôle du RSSI.*

CNIL. [En ligne] http://www.cnil.fr.

d'information, Direction centrale de la sécurité des systèmes. 2003. *Expression des Besoins et Identification des Objectifs de Sécurité.* 2003.

DCSSI. [En ligne] http://www.ssi.gouv.fr/fr/bonnes-pratiques/principes-generaux/.

Hélène Bienfait; Céline Glineur; HAPSIS. *La sensiblisation: Pourquoi, Pour qui, Comment?*

IBM. [En ligne] http://www-935.ibm.com/services/fr/igs/pdf/securite_attaques_internes.pdf.

ICSI. [En ligne] http://www.icsi-eu.org/francais/dev_cs/developper-culture securite.pdf.

IGICI. [En ligne] www.igici.ci .

ISCI. [En ligne] www.icsi-eu.org/.

—. *Politique de l'ICSI pour développer une culture de la sécurité.*

ISO/IEC. 2005. *Information Technology Code of practice for information security management.* 2005. 17799.

Laurent Bloch, Christophe Wolfhugel. *Sécurité Informatiques: principes et méthodes.*

Microsoft. [En ligne] http://msdn.microsoft.com/fr-fr/library/t4ahd590(v=vs.80).aspx.

SECUSYS. [En ligne] www.secusys.com.

Simon, Kevin Mitnick et William L. *L'art de la supercherie.* s.l. : éditions Campus Press.

INDEX

V

W

Suivre l'auteur du book sur les réseaux sociaux