Introduction

Depuis l'Antiquité, l'Homme cherche à se sécuriser, il confère à ce besoin une importance capitale. Une importance qui se justifie par la volonté de se protéger contre les facteurs externes.

Avec l'apparition de l'informatique et sa pleine expansion, le problème de sécurité s'impose, c'est un nouveau problème multiaxes qui touche à l'ensemble des activités, des intervenants, des équipements qui concernent le domaine de l'informatique.

La sécurité admet plusieurs axes :

– le premier axe concerne l'aspect énergétique, il consiste à assurer et maintenir l'énergie nécessaire pour le bon fonctionnement du système informatique ;

– le deuxième axe s'intéresse à l'aspect physique, il consiste à sécuriser physiquement les locaux et l'infrastructure matérielle du système informatique, en l'occurrence les systèmes de communication câblés et sans fil, les équipements intermédiaires d'interconnexion, de transmission et de sécurité (répéteurs, concentrateurs, commutateurs, routeurs, *firewalls*, etc.), des équipements terminaux de traitement aussi bien des stations de travail que des serveurs. La sécurité physique permet de sécuriser le système informatique contre les facteurs naturels tels que l'inondation, l'incendie, etc. et humains tels que le vol ;

– le troisième axe est un aspect propre à la sécurité informatique contrairement aux deux premiers qui s'appliquent dans n'importe quel domaine industriel nécessitant de l'énergie et admettant un patrimoine matériel critique. Cet axe a pour objectif de résoudre les problèmes spécifiques de la sécurité relatifs à la

technologie de l'informatique afin d'assurer un accès sûr et d'interdire l'accès non autorisé d'une part et de protéger le patrimoine logiciel et les données, contre toute utilisation non autorisée, d'autre part.

Bien qu'il n'existe pas une solution radicale de sécurité toute prête à appliquer, les solutions de sécurité ne cessent de se développer mais restent toujours insuffisantes pour résoudre les problèmes de sécurité. Nous assistons à une bataille continue entre les responsables de sécurité d'une part et les attaquants, les pirates et les intrus d'autre part.

Cette bataille se manifeste par les groupes de travail de chacune des deux parties, c'est le cas du groupe Anonymous et des organismes internationaux qui s'intéressent à la sécurité.

Les attaquants ne cessent de chercher et d'identifier les failles, concevoir les moyens d'attaques appropriés qui exploitent les vulnérabilités en question et surmonter les contre-mesures qui peuvent éventuellement être déployées.

Ce défi nécessite de l'autre côté un investissement qui permet de mobiliser des moyens humains et matériels pour faire face aux attaques et aux actions malveillantes diversifiées qui menacent la sécurité d'un système informatique. Divers moyens organisationnels, intellectuels, matériels et logiciels de sécurité ont vu le jour et ne cessent de se développer en quantité et en qualité dans les dernières années.

La sécurité, bien qu'elle soit négligée par ignorance dans la majorité des cas, constitue un défi très important. Lever ce défi n'est pas une tâche simple faute d'absence de solution radicale ou d'une feuille de route claire et exacte à appliquer. La seule façon de garantir un minimum de sécurité, c'est à travers l'alliance de plusieurs mesures sociales, culturelles et techniques. Cependant, ces mesures de sécurité restent dynamiques et dépendantes des circonstances, on assiste à la nécessité d'une veille technologique qui permet d'effectuer perpétuellement les modifications et les correctifs nécessaires sur la politique de sécurité en vigueur.

L'intervention d'experts et de personnes externes représente une action de valeur et un facteur d'importance capitale pour la définition et l'évolution de la politique de sécurité. Cette intervention peut se matérialiser par les missions

d'audit sécurité qui s'effectuent au niveau de l'entreprise ou par l'intervention directe d'experts lors d'actions de *consulting* pour les PME/PMI.

Plusieurs recommandations d'ordre général doivent être appliquées afin de garantir le minimum nécessaire en matière de sécurité.

D'abord, le service ou la cellule de sécurité doit forcément figurer au niveau de l'organigramme de l'entreprise tout en allouant au responsable de ce service ou de cette cellule, qui doit posséder un minimum de culture en matière de sécurité, le pouvoir et les facilités logistiques d'intervention nécessaires.

De plus, miser sur l'ignorance des agents et des utilisateurs n'a jamais été une mesure de sécurité. Il fallait instaurer une culture en matière de sécurité à travers des cycles de formations bien étudiés qui touchent à l'ensemble du personnel (cadres et agents) d'une part et prévoir des chartes et des affiches d'autre part.

Finalement, il fallait appliquer les mesures techniques de sécurité nécessaires et qui dépendent du patrimoine informatique de l'entreprise, et ce en déployant les équipements et les logiciels appropriés et en appliquant les mesures de sécurité. Reste à signaler que cette dernière recommandation, bien qu'elle soit incontournable, peut être mise en cause, et voire même sans intérêt, si on néglige pour une raison ou une autre les deux premières recommandations.

Le problème de sécurité n'est pas un souci purement professionnel qui concerne uniquement les entreprises et les institutions, il s'agit d'une question sociale en premier lieu et qui concerne la famille et la société d'une façon générale. En effet, l'utilisation de l'informatique et l'accès à Internet a envahi la société et pose plusieurs défis notamment pour les enfants qui peuvent accéder à n'importe quelle information et être stimulés par les réseaux sociaux avec l'incapacité des parents pour les contrôler. Pour lever ce défi qui présente une gravité non négligeable, deux mesures de base sont nécessaires, culturelle et technique, à travers des tâches de sensibilisation en famille, à l'école, dans les médias en plus du déploiement des logiciels appropriés de contrôle parental.

Cet ouvrage s'intéresse à plusieurs sujets en relation avec la sécurité :

1) la mise en évidence du sujet de la sécurité en identifiant la problématique, en précisant l'importance, les services et les mécanismes ;

2) l'identification des failles et problèmes de sécurité, et ce qu'ils soient d'ordres culturels et humains aussi bien que matériels et techniques ;

3) la mise au point des solutions de sécurité sur le plan technique et organisationnel en l'occurrence les antivirus, les *firewalls*, les IDS et les différentes techniques de contrôle d'accès, d'authentification et de chiffrement ;

4) la sécurité des réseaux SDN et des réseaux de capteurs IoT/IoE qui sera abordée moyennant la spécificité de ces technologies ;

5) le management de la sécurité, en l'occurrence l'audit sécurité et la mise en place de la politique de sécurité.