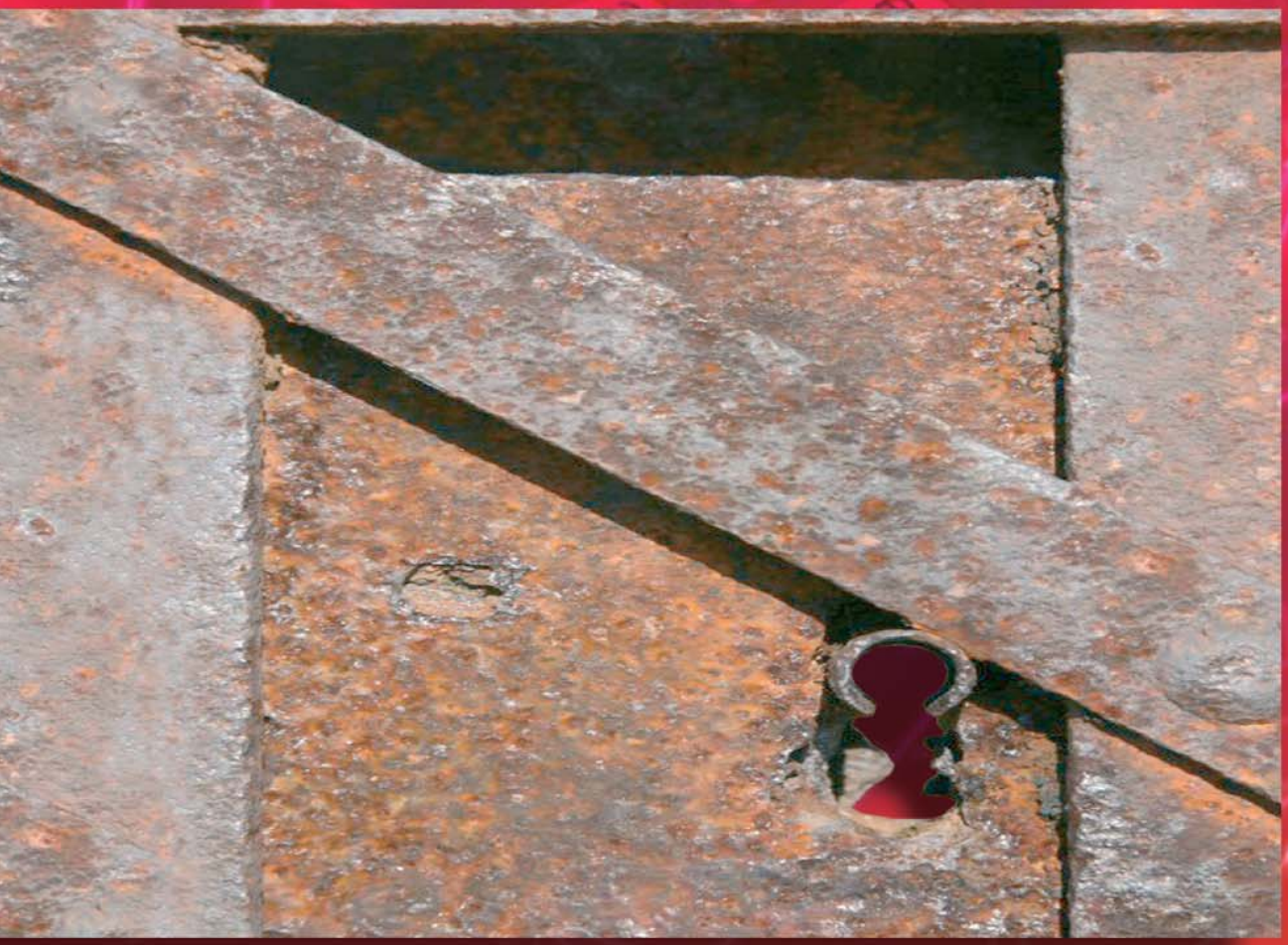
Union internationale des télécommunications

Guide de la cybersécurité pour les pays en développement



Union internationale des télécommunications

Union internationale des télécommunications

Guide de la cybersécurité pour les pays en développement

Union internationale des télécommunications

Les dénominations et classifications employées dans le présent rapport n'impliquent l'expression d'aucune opinion de la part de l'Union internationale des télécommunications concernant le statut juridique ou autre de tel ou tel territoire, ni l'acceptation ou l'approbation d'une quelconque frontière. Le terme «pays» utilisé dans le présent rapport désigne un pays ou un territoire.

Déni de responsabilité

Les références faites à des pays, sociétés, produits, initiatives ou directives spécifiques n'impliquent pas que l'UIT approuve ou recommande ces pays, sociétés, produits, initiatives et directives, de préférence à d'autres, de nature similaire, mais dont il n'est pas fait mention. Les opinions exprimées dans cette publication sont celles de l'auteur et n'engagent pas l'UIT.

PRÉFACE

Les technologies de l'information et de la communication (TIC) permettent de fournir des services de base dans les domaines, entre autres, de la télésanté, de la télééducation, du commerce électronique et de la cybergouvernance aux populations des pays en développement dans lesquels de nombreux citoyens n'ont toujours pas accès à des infrastructures physiques telles que les hôpitaux, les écoles ou les services publics de l'administration.

Les transactions électroniques entre médecins et patients, l'accès aux services publics administratifs en ligne et l'utilisation de l'internet pour vendre des biens et des services à des clients situés dans des zones éloignées sont désormais possibles grâce aux progrès réalisés dans le domaine des technologies de l'information et des télécommunications. Les applications offertes par les technologies de l'information et de la communication sont en passe de combler certaines difficultés d'accès aux services de base et de donner les moyens aux pays en développement de devenir des participants à part entière de la société de l'information.

Toutefois, on ne pourra profiter de tous les avantages offerts par la société de l'information qu'au prix d'un travail collectif de toutes les parties prenantes pour résoudre des problèmes tels que la prévention de la destruction des informations et données, la protection des données, l'authentification des transactions électroniques et la lutte contre la menace globale que représente le cybercrime. Le vol d'identité, l'envoi de messages non désirés, les techniques de «phishing», les logiciels malveillants tels que les chevaux de Troie, les vers ou les virus, se répandent par delà les frontières nationales, affectant les ordinateurs des utilisateurs à travers le monde.

Pour tirer profit des avantages offerts par la cybersécurité, les secteurs public et privé de tous les pays doivent avoir une compréhension commune des défis à relever. Il est essentiel que la communauté internationale poursuive ses efforts pour réduire la fracture de la connaissance entre les pays et à l'intérieur de ceux-ci dans cet important domaine.

Ce guide de référence a été conçu dans le but de fournir aux pays en développement une meilleure compréhension des principaux problèmes rencontrés actuellement en matière de cybersécurité, mais aussi pour promouvoir l'échange des meilleures pratiques, présenter des solutions mises en place dans d'autres pays et fournir des références dans ce vaste domaine.

J'espère que ce guide répondra aux besoins des utilisateurs, des responsables politiques, des régulateurs et des fournisseurs de services, en particulier dans les pays en développement, à l'heure où des solutions sont échafaudées pour profiter de tous les avantages qu'offrent les télécommunications et les technologies de l'information et de la communication au profit du développement social et économique.

Hamadoun I. Touré

Directeur
Bureau de développement des télécommunications

AVANT-PROPOS

La Conférence mondiale de développement des télécommunications a chargé le BDT, à travers le Programme «cyberstratégies et cyberservices/applications», de concevoir des outils visant à faciliter l'échange d'informations sur les meilleures pratiques, les technologies et les questions de politique générale. C'est dans ce cadre, et afin de répondre à l'une des priorités de ce Programme qui consiste à «renforcer la sécurité et la confiance dans l'utilisation des réseaux publics pour les cyberservices/applications», que le guide de la cybersécurité pour les pays en développement a été préparé.

Ce guide a été élaboré dans le but de fournir un outil aux pays en développement pour leur permettre de mieux comprendre certains enjeux liés à la sécurité des technologies de l'information, ainsi que des exemples de solutions mises en place par d'autres pays pour faire face à ces problèmes. Il cite également des références permettant d'obtenir de plus amples renseignements sur le sujet de la cybersécurité. Ce guide ne constitue pas un document ou un rapport exhaustif sur le sujet, mais vise à souligner les principaux problèmes que rencontrent actuellement les pays qui veulent bénéficier des avantages offerts par la société de l'information.

Son contenu tient compte des besoins des pays en développement et des pays les moins avancés dans l'utilisation des technologies de l'information et de la communication pour offrir des services de bases dans différents secteurs, et de l'importance de développer la capacité locale et une conscience accrue de toutes les parties prenantes.

Lors de l'élaboration du contenu et afin d'éviter toute duplication dans le traitement des thèmes, les travaux déjà réalisés par le Commission d'études 17 de l'UIT-T et les autres travaux et publications relatifs à ce domaine ont été dûment pris en compte.

Ce guide a été élaboré par Mme Solange GHERNAOUTI-HELIE, Professeur à l'Université de Lausanne, qui a travaillé en tant qu'expert UIT en collaboration étroite avec et sous la supervision de M. Alexander NTOKO, Chef de l'Unité des e-stratégies du BDT.

RÉSUMÉ

Enjeux de société, enjeux économiques, enjeux politiques, enjeux humains, qu'elle soit dénommée sécurité de l'informatique et des télécoms ou cybersécurité, la sécurité informationnelle touche à la sécurité du patrimoine numérique et culturel des individus, des organisations et des nations. Enjeux complexes dont la satisfaction passe par une volonté politique de définir et de réaliser une stratégie de développement des infrastructures et services du numérique (e-services) qui intègre une stratégie pluridisciplinaire de la cybersécurité cohérente, efficace et contrôlable.

Obtenir un niveau de sécurité informatique suffisant pour prévenir les risques technologique et informationnel est primordial pour le bon fonctionnement des Etats et des organisations. En effet, l'adoption des technologies du numérique, la dépendance des organisations et des Etats à ces mêmes technologies et l'interdépendance des infrastructures critiques, introduisent un degré de vulnérabilité non négligeable dans le fonctionnement normal des Institutions. Ceci peut mettre en péril leur pérennité ainsi que la souveraineté des Etats.

L'objet de la cybersécurité est de contribuer à préserver les forces et les moyens organisationnels, humains, financiers, technologiques et informationnels, dont se sont dotées les Institutions, pour réaliser leurs objectifs. La finalité de la sécurité informatique est de garantir qu'aucun préjudice ne puisse mettre en péril leur pérennité. Cela consiste à diminuer la probabilité de voir des menaces se concrétiser, à en limiter les atteintes ou dysfonctionnements induits, et autoriser le retour à un fonctionnement normal à des coûts et des délais acceptables en cas de sinistre.

La démarche de cybersécurité est un projet de société dans la mesure où chacun est concerné par sa réalisation. Sa validité sera renforcée si une cyberéthique, un comportement cohérent vis-à-vis des technologies de l'information est développée et si une véritable politique de sécurité stipule ses exigences de sécurité envers les utilisateurs (acteurs, partenaires, prestataires) des nouvelles technologies.

Pour mettre en place une démarche de cybersécurité, il est important de pouvoir identifier correctement les valeurs et les biens à protéger afin de circonscrire le périmètre de sécurité à mettre en place pour les protéger efficacement. Ceci implique une approche globale, pluridisciplinaire et systémique de la sécurité. La cybersécurité n'est pas compatible avec un monde libertaire, fluide et non contrôlé. Il faut établir des grands principes d'éthique, de responsabilité, de transparence au travers d'un cadre légal approprié et mettre en vigueur des règles du jeu réalistes. Celles-ci doivent être applicables non seulement localement mais aussi par l'ensemble de la communauté internationale et compatibles avec les directives internationales existantes.

Afin de ne pas contribuer à favoriser le développement de la criminalité, les infrastructures de télécommunication mises en place doivent intégrer des mesures de sécurité adaptées tant sur le plan technique que juridique. Les cyberattaques prennent diverses formes – prise de contrôle clandestine d'un système, déni de service, destruction ou vol de données sensibles, *hacking* (piratage de réseau de télécommunication), *cracking* (craquage de protections logicielles des programmes), *phreaking* (sabotage, prise de contrôle de centraux téléphoniques), etc. – et ont toutes des conséquences négatives pour les organisations ou individus qui en sont victimes.

Considérées comme un système, les télécommunications (infrastructures et services) répondent à une problématique de sécurité peu différente de celle des ressources informatiques, dont la résolution répond aux mêmes impératifs techniques, organisationnels et humains. Protéger les informations lors de leur transfert est nécessaire mais ne suffit pas car ces dernières sont tout aussi vulnérables, sinon plus, lorsqu'elles sont traitées et mémorisées. Ainsi, la cybersécurité doit s'appréhender d'une manière globale. Des solutions sécuritaires d'ordre uniquement technologique ne peuvent pas suppléer à un

manque de gestion cohérente et rigoureuse des besoins, mesures, procédures et outils de la sécurité. La prolifération désordonnée d'outils de sécurité ne peut qu'entraver l'usage, qu'alourdir l'exploitation ou encore dégrader les performances des ressources informatiques. La maîtrise de la sécurité informatique est une question de gestion dont les outils et les services de sécurité constituent une partie liée à l'administration opérationnelle des systèmes. Ainsi par exemple, chiffrer des données pour les rendre incompréhensibles lors de leur transmission ne sert à rien, si par la suite, elles sont stockées de manière non sécurisée. De même, la mise en place d'un *firewall* est de peu d'utilité si des connexions peuvent s'établir sans passer par ce système.

Le développement des activités basées sur le traitement de l'information permettant une réduction de la fracture digitale passe par la mise à disposition:

- d'infrastructures informationnelles fiables et sécurisées (accessibilité, disponibilité, sûreté de fonctionnement et continuité des services garanties);
- de politiques d'assurance;
- d'un cadre légal adapté;
- des instances de justice et de police compétentes dans le domaine des nouvelles technologies et capables de coopérer au niveau international avec leurs homologues;
- d'outils de gestion du risque informationnel et de gestion de la sécurité;
- d'outils de mise en œuvre de la sécurité qui permettent de développer la confiance dans les applications et services offerts (transactions commerciales et financières, e-santé, e-gouvernement, e-vote, etc.) et dans les procédures qui permettent le respect des droits de l'Homme notamment pour ce qui concerne les données à caractère personnel.

La maîtrise du patrimoine numérique informationnel, la distribution de biens intangibles, la valorisation des contenus ou la réduction de la fracture numérique, sont autant de problèmes d'ordre économique et social, dont la résolution ne pourra être réduite à la seule dimension technologique de la sécurité informatique. Ainsi, en apportant une réponse adéquate aux dimensions humaine, juridique, économique et technologique des besoins de sécurité des infrastructures numériques et des utilisateurs, la confiance pourrait s'instaurer et générer un développement économique profitable à tous les acteurs de la société.

PARCOURS DE LECTURE

En guise d'introduction à la cybersécurité, l'accent est mis sur ce qui a changé avec les technologies du numérique, la dématérialisation des informations et l'usage extensif des réseaux de télécommunication. Les enjeux pour l'évolution des sociétés sont présentés pour introduire la notion d'impératif de sécurité informatique et télécom (cybersécurité).

La section une de ce manuel s'intéresse principalement aux besoins et éléments de solution de la cybersécurité. Ainsi, le contexte de la sécurité des infrastructures de communication est analysé à la lumière du constat de la vulnérabilité et de l'état d'insécurité associé aux technologies de l'information et des communications. En tirant partie des enseignements issus des meilleures pratiques, de la réalité quotidienne de la sécurité du monde de l'internet et de l'expérience acquise par la communauté internationale, les besoins en termes de cybersécurité pour les pays en développement sont identifiés.

La cybersécurité est analysée selon ses dimensions managériales, politique, économique, sociale juridique et technologique. Sont identifiées des recommandations génériques à respecter lors de la mise à disposition d'infrastructures de télécommunication afin de maîtriser les risques, qu'ils soient d'origine criminelle ou non, et pour contribuer à développer la confiance envers les e-services, moteurs du développement économique.

La section deux adresse la problématique de la maîtrise de la cybercriminalité. Elle traite des éléments qui favorisent l'expression de la criminalité afin de mettre en évidence les limites des solutions actuelles de sécurité et de lutte contre la cybercriminalité ainsi que la complexité et de l'envergure du problème à résoudre.

Les différents délits et crimes réalisables via l'internet sont présentés, notamment sous l'angle de la criminalité économique. Une analyse des comportements criminels, comme le profil des cybercriminels, ainsi que les caractéristiques générales des cyberattaques et des programmes malveillants illustrent cette partie. Des lignes directrices sont identifiées pour se préparer à la menace d'origine cybercriminelle.

La section trois, après avoir rappelé les fondamentaux du monde des télécommunications, propose une approche fonctionnelle ainsi qu'une mise en perspective critique des outils de la sécurité des infrastructures.

Une approche globale de la cybersécurité qui intègre les différents aspects du droit des nouvelles technologies ainsi que quelques perspectives de développent pour la mise en place de solutions de sécurité des infrastructures de communication sont données en section quatre.

Un glossaire des termes de la sécurité ainsi que diverses références et documents concluent ce guide de la cybersécurité.

REMERCIEMENTS

Le Bureau de développement des télécommunications de l'UIT souhaite remercier Madame le Professeur Solange Ghernaouti–Hélie ainsi que tous les membres de son équipe pour leur soutien, notamment MM. Mohamed Ali Sfaxi et Igli Tashi, Mmes Sarra Ben Lagha et Hend Madhour, ainsi que M. Arnaud Dufour (consultant en stratégie internet).

Par ailleurs, ce manuel a bénéficié des informations et études fournies par divers organismes et tout particulièrement par le Clusif (Club de la sécurité informatique français) et le Cert (*Computer Emergency and Response Team*), que nous tenons à remercier.

Enfin, l'élaboration de ce manuel n'aurait pas été possible sans l'excellente coopération des membres de l'Unité e-stratégies, en particulier M. Alexander Ntoko. Nous souhaitons également remercier Mme Renée Zbinden Mocellin (Division de la production des publications de l'UIT) et son équipe pour la production de ce guide.

TABLE DES MATIÈRES

Page

Page

Page

Page

Page

Page

SECTION I

CONTEXTE DE LA CYBERSÉCURITÉ
ENJEUX ET ÉLÉMENTS DE SOLUTION

Chapitre I.1 – Cyberespace et société de l'information

I.1.1 Numérisation

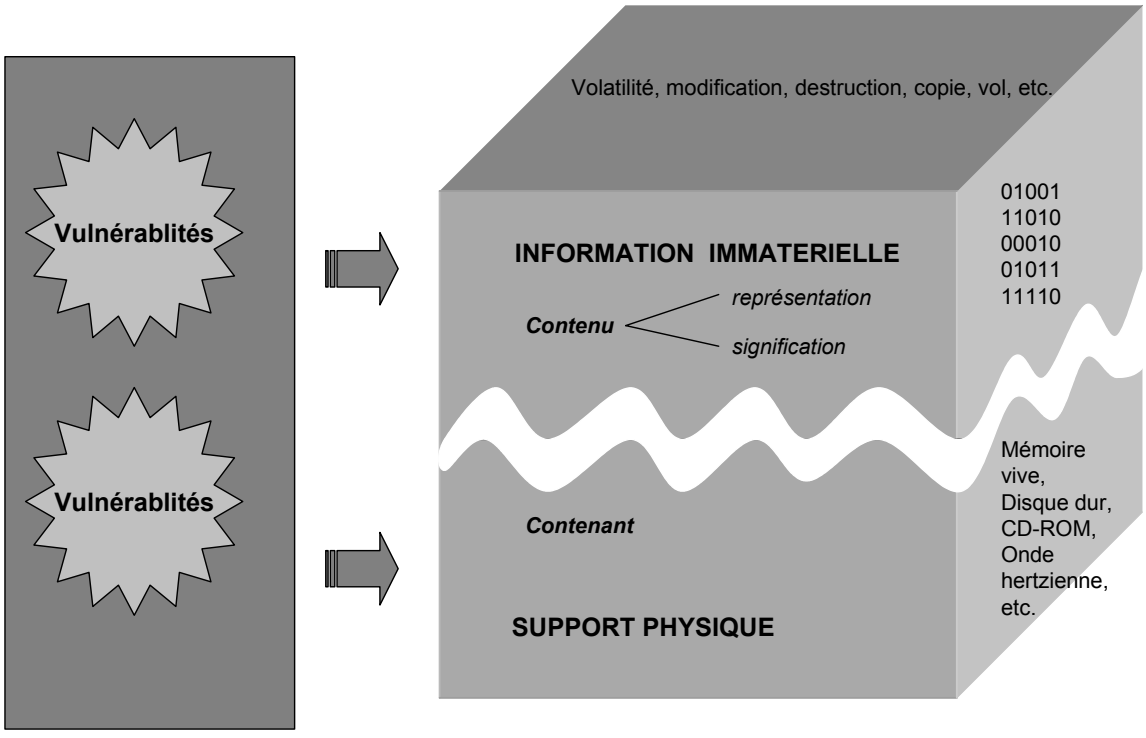
Les technologies informatiques transforment notre façon de concevoir et de réaliser l'ensemble des activités humaines. Elles induisent des modifications structurelles importantes car tous les *objets* sont devenus manipulables électroniquement au travers de l'information les modélisant.

I.1.1.1 Information numérique

La technique de numérisation crée une image digitale ou double virtuel ou encore double numérique des entités existantes. Quelle que soit sa nature (voix, données, image), toute information est numérisable et possède une représentation homogène, c'est-à-dire uniforme.

L'information n'est plus associée physiquement à son contenant, c'est-à-dire à son support de représentation et de stockage. Sa valeur ajoutée provient directement de l'information elle-même (contenu ou content); en effet, les coûts de diffusion et de mémorisation de l'information sont peu élevés par rapport à ceux de sa conception (Figure I.1). De plus, les données peuvent être localisées et traitées simultanément à plusieurs endroits. Ainsi, étant dupliquables à l'infini et de façon parfaite, la notion de données «originales» perd son sens, ce qui peut poser des problèmes relatifs à la notion de protection des droits d'auteur.

Figure I.1 – Dématérialisation et information numérique



I.1.1.2 Technologies numériques

Les technologies numériques en uniformisant la production, le traitement et le transfert des données permettent une continuité numérique de toute la chaîne d'information. Cette convergence numérique, associée aux techniques de compression des données, favorise les synergies entre l'informatique, les télécommunications et le monde de l'audiovisuel, comme le révèle le phénomène internet. On remarque alors que la véritable révolution technologique s'est produite grâce à la numérisation de l'information, dont les conséquences dépassent largement le cadre des télécommunications.

Toutes les disciplines, tous les domaines d'activités, tous les métiers se trouvent affectés par cette nouvelle dimension de traitement de l'information. La détermination de la valeur aussi bien que les modes de production, depuis la conception des produits jusqu'à leur distribution, se sont ces dernières années progressivement modifiés. Cela a conduit à une réorganisation des chaînes de valeur entre les différents acteurs économiques.

I.1.1.3 Infrastructures et contenu

La conquête du contrôle de la chaîne numérique de l'information, c'est-à-dire de l'infrastructure et du contenu, constitue désormais l'enjeu dominant du XXII^{e} siècle. Ce nouveau marché, ouvert à tous, se caractérise par une mobilisation sans précédent de tous les acteurs de l'économie mondiale (opérateurs de télécommunication, câblo-opérateurs, fabricants de matériels et logiciels, chaînes de télévision, etc.).

La concurrence effrénée et la redistribution des zones d'action et des rôles, afin d'offrir des services intégrés couvrant la planète, constituent le nouvel enjeu économique des organisations actuelles.

Lorsque Gutenberg imprima son premier livre, il n'imaginait pas les retombées industrielles de son invention, lesquelles furent celles des premiers pas vers l'automatisme industriel. Il en est de même, lorsque vers la fin des années 60, universitaires et militaires américains mirent en œuvre, pour des motivations fort différentes et apparemment contradictoires, un réseau de communication qui donna naissance au réseau internet. Tout comme au XV^{e} siècle, les conséquences de leur création leur échappèrent. Aujourd'hui, le cyberespace internet marque le passage de des sociétés à l'ère informationnelle.

I.1.2 Révolution informationnelle

La révolution informationnelle bouleverse le traitement et la conservation de l'information. Elle modifie le mode de fonctionnement des organisations et de la société toute entière. Bien qu'elle ne soit pas la seule innovation technique de ces dernières années, elle est particulièrement importante dans la mesure où elle touche à la manipulation de l'information et donc de la connaissance. Son impact se porte sur les mécanismes de génération et de transmission du savoir, ce qui permet de penser la révolution informationnelle source d'innovation future dont les pays en développement ne devraient pas être exclus.

L'évolution des technologies de l'information et des télécommunications conduit à une véritable révolution dans le mode de pensée des échanges tant économiques que sociaux ou culturels. Ceci établit également un nouveau modèle informatique centré sur le réseau; modèle dans lequel il est nécessaire de maîtriser la sécurité de la circulation des informations, afin d'autoriser le développement de nouvelles applications qui rendront les organisations encore plus efficaces. Aucune forme de vie économique ne peut exister sans échanges et interactions entre ses diverses composantes, aucun échange d'information ne peut s'envisager sans l'assurance d'un certain niveau de sécurité et aucun service ne peut être considéré sans qualité de service. Remarquons toutefois, que la réussite d'une communication dépend de la capacité des interlocuteurs à dominer les contraintes techniques et à gérer les rites associés à tout échange d'informations.

I.1.2.1 Innovation et développement

Seules les capacités d'innovation et d'adaptation rapide, sous-tendues par un système d'information performant et sécurisé, permettent aux organisations et aux Etats de rester pérennes et de se positionner comme acteur du nouvel environnement concurrentiel.

De nouveaux territoires d'activités se sont ouverts par la diversification des télécommunications et les possibilités offertes par l'informatique étendue qui doivent aussi profiter aux pays en développement.

Les évolutions technologiques et économiques possibles à partir de déploiement d'infrastructures informatiques fiables sont porteuses de promesses pour les peuples. En contrepartie, elles introduisent une dimension de complexité technologique et de gestion sans précédent. Ceci peut conduire à un risque technologique majeur qu'il faut savoir maîtriser, faute de quoi toute idée d'évolution n'aurait aucun sens. Un risque technologique: défaillance des systèmes de traitement de l'information et des communications liée à un dysfonctionnement accidentel ou provoqué. Au risque technologique est corrélé le risque informationnel qui exprime une atteinte à la capacité d'exploiter les informations de l'organisation.

Il est important de relever que si l'accès à l'informatique est large et en croissance, une frange non négligeable de la population se trouve exclue de la révolution informationnelle. Cet état de fait trouve ses justifications à différents niveaux aussi bien culturels que financiers, et peut dans certains cas être lié à des difficultés de base comme l'illettrisme. Démocratiser les technologies de l'information par des actions de formation et l'éducation ont, dans ce domaine plus que dans tout autre, un rôle à jouer dans la lutte contre l'info-exclusion. Cela nécessite également de repenser les interfaces de communication afin de desservir aux mieux les populations et respecter les diversités culturelles contextuelles. L'outil informatique doit s'adapter aux environnements humains dans les lesquels il doit s'intégrer et nom imposer un nouvel ordre communicationnel.

I.1.2.2 Accompagner la révolution informationnelle

Les technologies de l'information et de communication sont, comme toute technique, conçues et mises en œuvre dans un espace temporel et géographique déterminé, révélant normalement un certain équilibre de la société. Il est de la responsabilité des hommes d'accompagner la révolution informationnelle en la dotant d'outils, de procédures, de législation et d'une éthique sécuritaire satisfaisant à sa réalisation, et correspondant aux attentes et aux besoins de la société.

On ne peut que constater qu'il existe une multitude de réglementations incomplètes relatives à l'utilisation des différents médias de communication, aux libertés d'émission et de réception de messages issues de l'UIT (Union internationale des télécommunications), de l'Unesco, de l'ONU, de l'OCDE, du Conseil de l'Europe, etc. Un décalage important s'est créé entre la situation actuelle concernant le développement et l'usage des technologies de l'information et des communications, et l'état des règlements. Un cadre juridique approprié doit donc être mis en place pour tenir compte notamment de l'aterritorialité des réseaux comme internet, des problèmes de responsabilité, de respect de la vie privée et de la propriété. L'évolution technologique doit être associée à une évolution d'ordre social, politique et juridique. Ces quelques regards jetés sur l'ère informationnelle relèvent l'importance des enjeux de sa maîtrise, du rôle prépondérant des télécommunications dans sa réalisation et d'un besoin de sécurité qui ne doit pas être un frein au développement.

Le passage à l'ère informationnelle révèle l'importance des technologies de l'information et de leur maîtrise. En considérant les dimensions nouvelles qu'elles introduisent sur les plans techniques et socio-économiques, la nécessité d'assurer la sécurité des systèmes et infrastructures informatiques et de télécommunications, est devenue fondamentale. Elle souligne le caractère stratégique et critique de la gestion et de la mise en œuvre de la cybersécurité, tant pour les Etats, les organisations que pour l'individu.

Dans la mesure où les Etats ont effectué des efforts financiers, matériels et humains importants pour réaliser leur infrastructure informatique et de télécommunication, il est primordial qu'ils se dotent des moyens permettant de les sécuriser, de les gérer et de les contrôler.

Chapitre I.2 – Cybersécurité

I.2.1 Contexte de la sécurité des infrastructures de communication

On assiste de nos jours à une prise en considération croissante des besoins de maîtrise des risques informatiques opérationnels du fait de l'usage extensif des nouvelles technologies, de l'existence d'une infrastructure informationnelle globale et de l'émergence de nouveaux risques.

La transformation des sociétés en société de l'information autorisée par l'intégration des nouvelles technologies dans toutes les activités et infrastructures accroît la dépendance des individus, des organisations et des Etats aux systèmes d'information et aux réseaux. Cela constitue un risque majeur qui doit être adressé comme un risque sécuritaire.

Les pays en développement sont confrontés à la problématique de la nécessité de faire partie de la société de l'information en prenant en considération le risque de leur dépendance vis-à-vis des technologies et des fournisseurs de ces technologies et en pensant que la fracture digitale existante ne doit pas se doubler d'une fracture sécuritaire encore moins d'une dépendance plus forte à des entités qui contrôleraient leurs besoins et moyens de sécurité des technologies de l'information[1].

Les infrastructures de télécommunication et les services et activités qu'elles permettent de développer et de générer doivent être pensés, conçues, mise en place et gérées en termes de sécurité. La sécurité est la pierre angulaire de toute activité et doit être vue comme un service permettant de créer d'autres services et de générer de la valeur (e-gouvernement, e-santé, e-éducation, etc.). Au-delà des technologies[2]. Or jusqu'à présent, les outils de communication basiques mis à disposition, n'intègrent pas des moyens suffisants et nécessaires à la réalisation ou à la garantie d'un niveau minimal de sécurité.

Les systèmes informatiques mis en réseau sont des ressources accessibles à distance et deviennent des cibles potentielles d'attaques informatiques. Cela accroît les risques d'intrusion des systèmes et offre un terrain favorable à la réalisation, à la propagation des attaques et des délits. Au-delà des systèmes attaqués ce sont les informations qu'ils manipulent qui sont convoitées (Figure I.2). Les attaques portent atteintes à la capacité à traiter, sauvegarder, communiquer le capital informationnel, aux valeurs immatérielles et aux symboles, aux processus de production ou de décision de ceux qui les possèdent. Les systèmes informatiques introduisent un risque opérationnel dans le fonctionnement des institutions qui les possèdent.

Ainsi, les réseaux de télécommunication et l'ouverture des systèmes posent des problèmes de sécurité informatique complexes et multiformes, relativement difficiles à maîtriser et qui peuvent avoir des conséquences et impacts critiques pour le fonctionnement des organisations et des Etats. De la capacité à maîtriser la sécurité des informations, des processus, des systèmes, des infrastructures dépend les facteurs critiques de succès des économies.

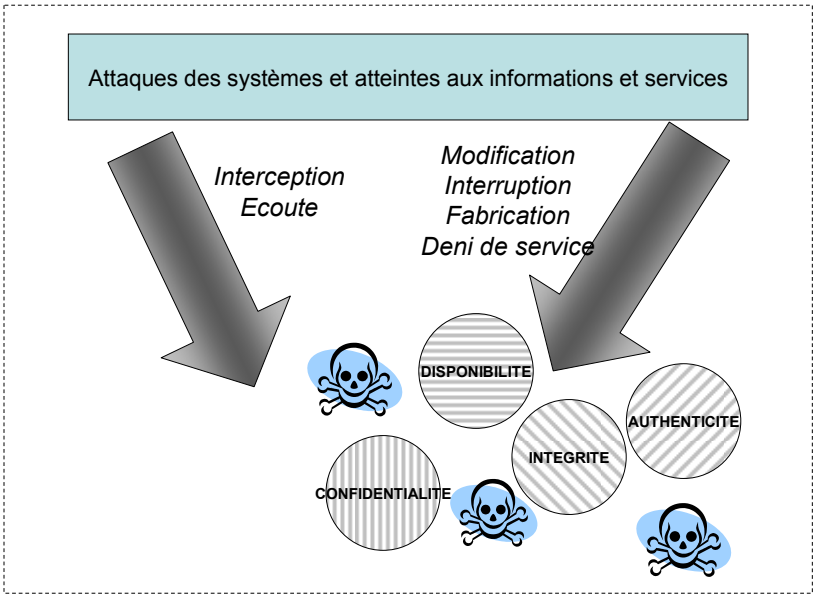
L'interconnexion extensive des systèmes, l'interdépendance des infrastructures, l'augmentation de la dépendance aux technologies du numérique, des menaces et des risques, nécessite de doter les individus, les organisations, et les Etats de mesures, procédures et outils qui autorise une meilleure gestion des risques technologique et informationnel. Les enjeux de la maîtrise des risques technologiques sont ceux du XXI^{e} siècle et sont à appréhender de manière globale au niveau internationale en intégrant dans la démarche sécuritaire des pays en développement.

---

1 S. Ghernaouti-Hélie: «From digital divide to digital unsecurity: challenges to developp and deploy an unified e-security framework in a multidimensional context». International cooperation and the Information Society, chapitre de l'annuaire Suisse de politique de développement. Iued publications. Genève, Novembre – 2003.

2 A. Ntoko: «Mandate and activities in cybersecurity – ITU-D». WSIS Thematic meeting on cybersecurity. ITU – Genève 28 juin – 1er juillet 2005.

Figure I.2 – Attaques des systèmes et atteintes à la sécurité des ressources



Ce n'est pas suffisant de mettre à disposition des points d'accès aux réseaux de télécommunication, il est impératif de déployer des infrastructures et des services informatiques fiables, maintenables, robustes et sécurisés, en respect des droits fondamentaux des personnes et des Etats. La protection des systèmes et des valeurs informations doit être complémentaire et en harmonie avec la protection des individus et de leur intimité numérique (*privacy*)

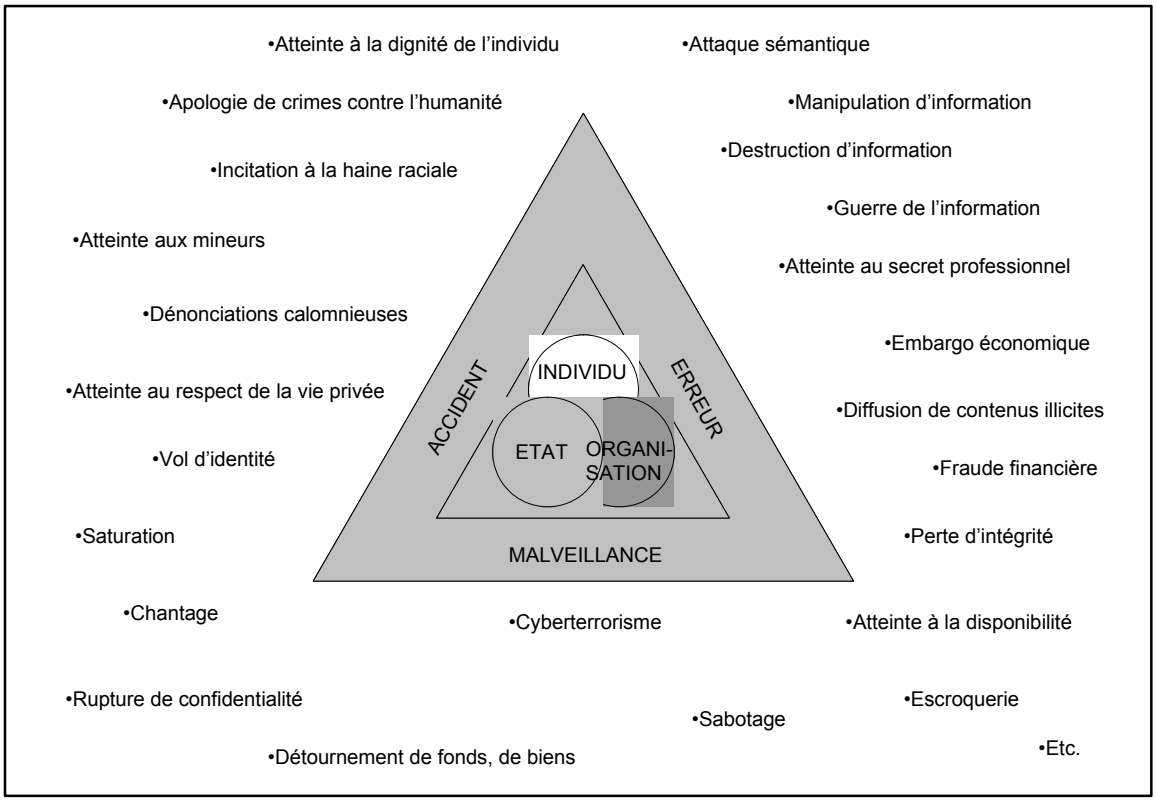
Entrer dans la société de l'information sans risque excessif et en tirant partie des expériences issues des pays développés, sans pour autant que la cybersécurité constitue un facteur supplémentaire d'exclusion, sont de nouveaux défis des pays en développement.

I.2.2 Enjeux de la cybersécurité

Enjeux de société, enjeux économiques, enjeux politiques, enjeux humains, qu'elle soit dénommée sécurité de l'informatique et des télécoms ou cybersécurité, la sécurité informationnelle touche à la sécurité du patrimoine numérique et culturel des individus, des organisations et des nations (Figure I.3). Enjeux complexes dont la satisfaction passe par une volonté politique de définir et de réaliser une stratégie de développement des infrastructures et services du numérique (e-services) qui intègre une stratégie de cybersécurité cohérente, efficace et contrôlable. Celle-ci se doit s'inscrire dans une approche pluridisciplinaire et des solutions d'ordre éducative, juridique, et managérial et technique doivent être mise en place. Ainsi, en apportant une réponse adéquate aux dimensions humaine, juridique, économique et technologique des besoins de sécurité des infrastructures numériques, la confiance pourrait s'instaurer et générer un développement économique profitable à tous les acteurs de la société.

La maîtrise du patrimoine numérique informationnel, la distribution de biens intangibles, la valorisation des contenus ou la réduction de la fracture numérique par exemple, sont autant de problèmes d'ordre économique et social, dont la résolution ne pourra être réduite à la seule dimension technologique de la sécurité informatique.

Figure I.3 – Différents niveaux de la cybersécurité: individus, organisations, Etats



Le développement des activités basées sur le traitement de l'information permettant une réduction de la fracture digitale passe par la mise à disposition:

- d'infrastructures informationnelles fiables et sécurisées (accessibilité, disponibilité, sûreté de fonctionnement et continuité des services garanties);
- de politiques d'assurance;
- d'un cadre légal adapté;
- des instances de justice et de police compétentes dans le domaine des nouvelles technologies et capables de coopérer au niveau international avec leurs homologues;
- d'outils de gestion du risque informationnel et de gestion de la sécurité;
- d'outils de mise en œuvre de la sécurité qui permettent de développer la confiance dans les applications et services offerts (transactions commerciales et financières, e-santé, e-gouvernement, e-vote, etc.) et dans les procédures qui permettent le respect des droits de l'Homme notamment pour ce qui concerne les données à caractère personnel.

L'objet de la cybersécurité est de contribuer à préserver les forces et les moyens organisationnels, humains, financiers, technologiques et informationnels, dont se sont dotées les Institutions, pour réaliser ses objectifs.

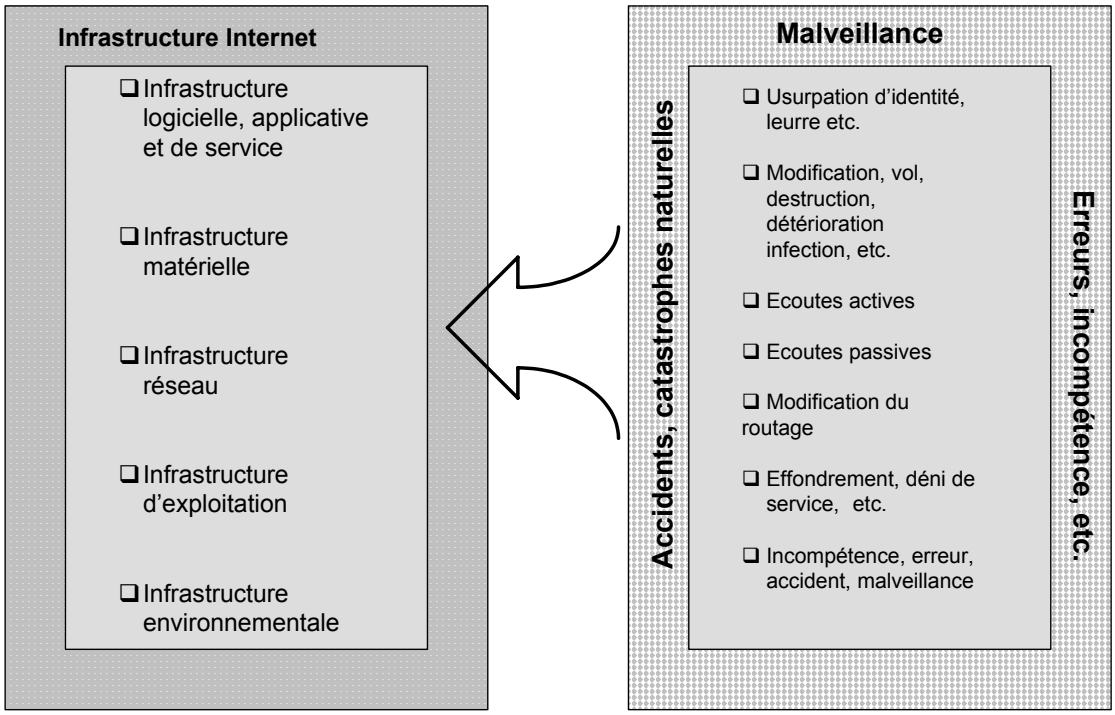
La finalité de la sécurité informatique est de garantir qu'aucun préjudice ne puisse mettre en péril la pérennité de l'organisation. Cela consiste à diminuer la probabilité de voir des menaces se concrétiser, à en limiter les atteintes ou dysfonctionnements induits, et autoriser le retour à un fonctionnement normal à des coûts et des délais acceptables en cas de sinistre.

La démarche de cybersécurité est un projet de société dans la mesure où chacun est concerné par sa réalisation. Sa validité sera renforcée si une cyberéthique d'utilisation et de comportement vis-à-vis des technologies de l'information est développée et si une véritable politique de sécurité stipule ses exigences de sécurité envers les utilisateurs, acteurs, partenaires et prestataires de la sécurité des nouvelles technologies.

I.2.3 Constat de l'insécurité numérique

La réalité de l'insécurité des technologies de traitement de l'information et des communications trouve ses origines dans les caractéristiques des technologies de l'information et du monde virtuel. La dématérialisation des acteurs, les accès à distance, un relatif anonymat, les problèmes de conception, de mise en œuvre, de gestion, de contrôle de l'informatique et des télécoms, associés aux pannes, dysfonctionnements, erreurs, incompétences, incohérences ou encore aux catastrophes naturelles, confèrent *de facto* un certain niveau d'insécurité aux infrastructures informatiques (Figure I.4).

Figure I.4 – Infrastructure de l'internet et multiplicité de l'origine des problèmes



Dans ce contexte, les possibilités d'exploitation de ces vulnérabilités et de malveillance sont nombreuses[3].

La réalité de ces dernières: usurpation d'identité, leurre de systèmes, accès indus, exploitation frauduleuse des ressources, infection, détérioration, destruction, modification, divulgation, déni de service, vol, chantage, etc. met en évidence les limites des approches sécuritaires actuelles, tout en révélant paradoxalement, une certaine robustesse des infrastructures.

Quelles que soient les motivations des acteurs de la criminalité informatique celle-ci engendre toujours des conséquences économiques non négligeables et constitue dans sa dimension de cybercriminalité, un fléau grandissant, transfrontalier et complexe.

Bien que des solutions de sécurité existent, elles ne sont pas absolues et ne répondent le plus souvent qu'à un problème particulier dans une situation donnée. Elles déplacent le problème de sécurité ou reportent la responsabilité de la sécurité et de plus, elles nécessitent d'être sécurisées et gérées de manière sécurisée.

3 La cybercriminalité ainsi que les cyberattaques et cyberdélits sont développés en section II.

Force est de constater qu'elles ne répondent que peu ou prou à la dynamicité du contexte dans lequel elles doivent s'intégrer. Les technologies ne sont pas stables, les cibles sont mouvantes, le savoir-faire des malveillants évoluent ainsi que les menaces et les risques. Ceci fait que la pérennité des approches sécuritaires, comme le retour sur investissements de celles-ci, ne sont jamais garantis.

Il est constaté, que la démarche sécuritaire est souvent limitée à la mise en place des mesures, de réduction des risques pour les valeurs informationnelles des organisations par le plus souvent, une approche technologique seule. Or, l'approche sécuritaire doit s'appréhender dans toutes ses dimensions et doit également réponde aux besoins de sécurité des individus, notamment pour ce qui concerne la protection de leur vie privée et du respect de leurs droits fondamentaux. La cybersécurité doit être disponible pour tous et doit prendre en considération le besoin de protection des données à caractère personnel.

Des solutions de sécurité existent. Souvent d'ordre technologique, elles répondent avant tout à un problème particulier dans une situation donnée. Mais comme toute technologie, elles sont faillibles ou contournables. Elles déplacent le plus souvent le problème de sécurité et reportent la responsabilité sur une autre entité du système qu'elles sont censées protéger. De plus, elles nécessitent d'être sécurisées et gérées de manière sécurisée. Elles ne sont jamais ni absolues, ni définitives, en raison du caractère évolutifs du contexte de la sécurité du fait de la dynamicité de l'environnement (évolution des besoins, des risques, des technologies, des savoirs-faire des délinquants, etc.). Cela pose le problème de la pérennité des solutions mises en place. De plus, la diversité et le nombre de solutions peuvent créer un problème de cohérence globale de l'approche sécuritaire. En conséquence, la technologie ne suffit pas, elle doit être intégrée dans une démarche de gestion.

La diversité et la pluralité des acteurs (ingénieurs, développeurs, auditeurs, intégrateurs, juristes, investigateurs, clients, fournisseurs, utilisateurs, etc.), la diversité d'intérêt de visions d'environnements, de langages, rendent difficile la cohérence globale des mesures de sécurité. Or seule une appréhension globale et systémique des risques et des mesures de sécurité, une prise de responsabilité de l'ensemble des acteurs et intervenants contribuent à offrir le niveau de sécurité attendu pour réaliser en confiance, des activités via les technologies de l'information et des communications ainsi que la confiance dans l'économie numérique.

I.2.4 Enseignements à tirer

I.2.4.1 Diriger la sécurité

Depuis le début des années 2000, la prise en compte par les organisations des problèmes liés à la sécurité informatique s'est généralisée du moins dans les grandes structures. La sécurité est de moins en moins une juxtaposition de technologies hétérogènes de sécurité. Elle doit être vue et gérée comme un processus continu.

Le «gouvernement» ou «gouvernance» de la sécurité doit permettre de garantir que les mesures de sécurité sont optimales dans le temps et dans l'espace. Cette notion répond aux interrogations simples suivantes:

- Qui fait quoi, comment et quand?
- Quels sont les acteurs qui élaborent les règles, qui les définissent et les valident, qui les mettent en œuvre et qui les contrôlent?

I.2.4.2 Identifier et gérer les risques

La prise en compte de l'analyse des risques liés à l'informatique, aux télécommunications et au cyberespace, dans un processus de gestion de risques (*risk management*), guide la démarche de sécurité des infrastructures numériques. Le risque sécuritaire lié au technologies de l'information (risque informatique, informationnel ou technologique, quelque soit le nom retenu) doit être identifié, au même titre que tous les autres risques (risque stratégique, social, environnemental, etc.) auxquels doivent faire face les institutions.

Le risque informatique est un risque opérationnel qui doit être maîtrisé. La gestion des risques constitue le point de départ de l'analyse des besoins de sécurité qui permet la définition de la stratégie et de la politique de sécurité. Plusieurs questions se posent retenons entre autres, les suivantes:

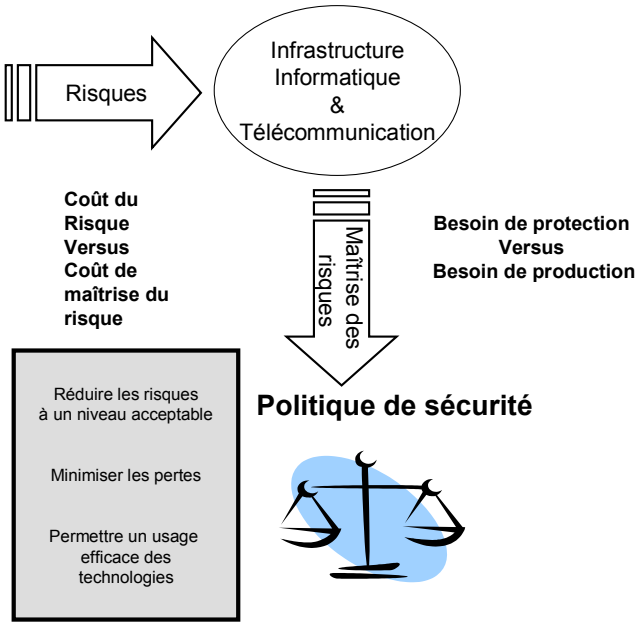
- Qui est responsable de l'analyse des risques, de la gestion des risques?
- Comment effectuer une telle analyse?
- Quels sont les outils et méthodologies disponibles?
- Quels sont leurs niveaux de fiabilité?
- Quelle importance à accorder aux résultats? Combien cela coûte?
- Faut-il externaliser cette fonction?
- Etc.

Un risque est un danger éventuel plus ou moins prévisible. Il se mesure à la probabilité qu'il se produise et aux impacts et dommages consécutifs à sa réalisation. Un risque exprime la probabilité qu'une valeur soit perdue en fonction d'une vulnérabilité liée à une menace, à un danger.

Un compromis entre le coût du risque et celui de sa réduction permet de déterminer le niveau de protection et les mesures de sécurité à mettre en œuvre (Figure I.5). En tout état de cause, il faut identifier les valeurs à protéger et pourquoi en fonctions des contraintes effectives et des moyens organisationnels, financiers, humains, techniques disponibles. Les mesures doivent être efficaces, et s'inscrire dans une logique d'optimalité / rentabilité.

Pour une organisation, la maîtrise des risques informatiques passe par la conception d'une stratégie, la définition d'une politique de sécurité et de sa réalisation tactique et opérationnelle.

Figure I.5 –Différents compromis pour la maîtrise des risques: un choix politique



I.2.4.3 Définir une politique de sécurité

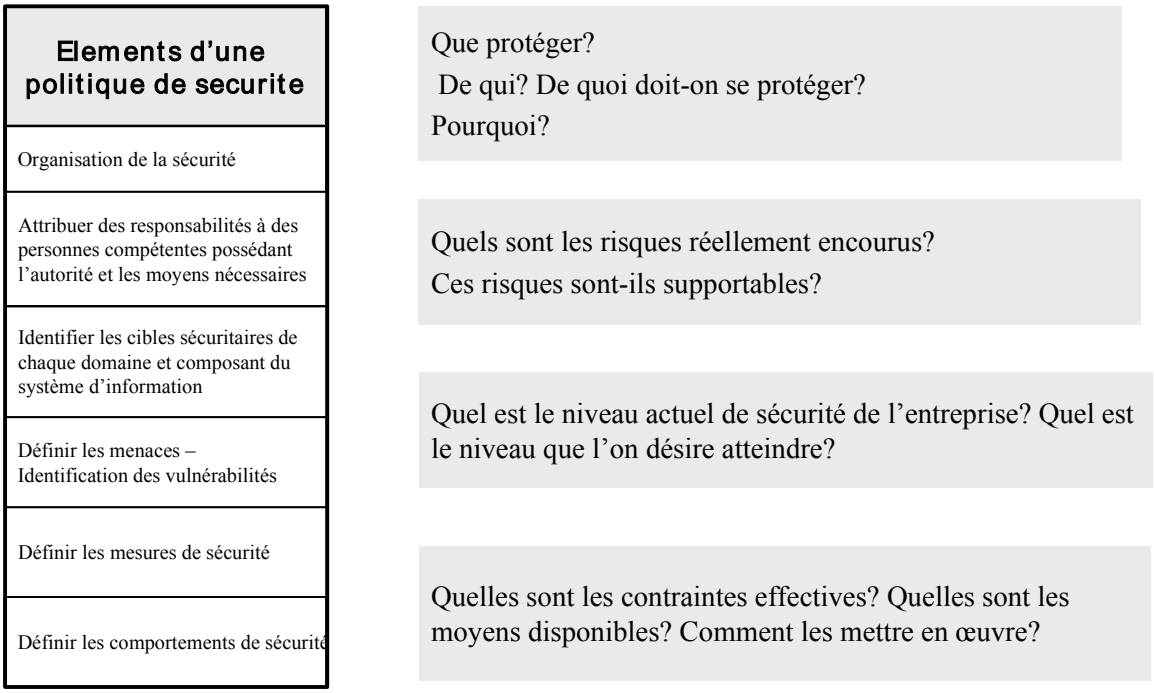
La politique de sécurité permet de traduire la compréhension des risques encourus et de leurs impacts, en des mesures de sécurité à implémenter. Elle facilite l'adoption d'une attitude préventive et réactive faces aux problèmes de sécurité et permet de réduire les risques et leurs impacts.

Sachant que le risque zéro n'existe pas et qu'il difficile de prévoir toutes les nouvelles menaces, il faut réduire les vulnérabilités des environnements et ressources à protéger car il est certain qu'une grande partie des problèmes de sécurité y trouvent leur origine.

Une politique de sécurité spécifie entre autres, les moyens, l'organisation, les procédures, les plans de défense et de réaction qui permettent une véritable maîtrise des risques opérationnel, technologique et informationnel.

La norme ISO 17799 propose un code de pratique pour la gestion de la sécurité. Elle peut être vue comme un référentiel permettant de définir une politique de sécurité, comme une liste de points de risques à analyser (*check list*), comme une aide à l'audit de la sécurité en vue ou non d'une procédure de certification ou encore, comme point de communication sur la sécurité. Diverses interprétations et réalisations de cette norme sont possibles. Son intérêt réside dans le fait que la norme aborde les aspects organisationnel, humain, juridique et technologique de la sécurité en rapport aux différentes étapes de conception, de mise en œuvre et de maintien de la sécurité. La version 2005 de cette norme (ISO/IEC 17799:2005)[4] met l'accent sur l'évaluation et l'analyse des risques, la gestion des valeurs et des biens ainsi que la gestion des incidents. On y remarque toute l'importance accordée à la dimension managériale de la sécurité.

Figure I.6 –Gérer la sécurité passe par la définition d'une politique de sécurité



L'efficacité d'une politique de sécurité ne se mesure pas au budget investi mais dépend de la politique de gestion du risque et de la qualité de l'analyse des risques (Figure I.6). Les risques varient notamment selon le secteur d'activité d'une organisation, de sa taille, de son image, de la sensibilité des systèmes, de leur environnement et des menaces associées et de son degré de dépendance au système d'information.

4 Les chapitres de la norme sont donnés en annexe de ce document.

La qualité de la sécurité informatique dépend, avant tout, de l'identification et de l'évaluation de la valeur du patrimoine informationnel, de la mise en œuvre opérationnelle de mesures de sécurité adaptées à partir d'une définition correcte d'une politique de sécurité et d'une gestion efficace.

I.2.4.4 Déployer des solutions

Divers types de mesures sont à déployer pour contribuer à sécuriser des infrastructures informatiques et télécoms. Il s'agit:

- d'éduquer, former, sensibiliser l'ensemble des acteurs à la cybersécurité;
- de mettre en place des structures qui permettent de fonctionner comme centre d'alerte et de gestion de crise au niveau national, de fédérer les moyens à mettre en œuvre pour les réaliser, les partager pour un ensemble de pays, pour une région;
- d'imposer des surveillances, des contrôles (par analogie aux contrôles mis en place sur les réseaux routiers);
- de développer les compétences d'une cellule de cyberpolice pouvant contribuer à une coopération internationale dans le domaine de la poursuite et de l'investigation du crime informatique;
- de développer des solutions technologiques pour ce qui concerne la gestion des identités, le contrôle d'accès, l'usage de plate-formes matérielle et logicielle sécurisées, les infrastructures de secours, les protocoles cryptographiques, la gestion opérationnelle.

I.2.5 Point de vue managérial

I.2.5.1 Gestion dynamique[5]

La prise en compte de la sécurité selon un processus de gestion dynamique et continu permet de faire face au caractère dynamique du risque et à l'évolution des besoins par une adaptation et optimisation continue des solutions. De la qualité de la gestion de la sécurité dépend le niveau de sécurité offert. La politique de cybersécurité est déterminée au niveau de l'état major de la structure concernée. Il existe autant de stratégies de sécurité, de politiques de sécurité, de mesures, de procédures ou de solutions de sécurité que d'organisations et de besoins sécuritaires à satisfaire à un moment donné.

Pour ne prendre qu'un exemple de dynamicité du contexte dans lequel s'inscrit la gestion de la sécurité retenons le processus de découverte et de correction des failles de sécurité. Celui se fait avec une publication périodique des correctifs (*patches* ou rustines de sécurité). Les lettres d'informations (*newsletters*) plus ou moins personnalisées permet de se tenir informer de la découverte des failles et de la manière d'y remédier. S'il veut maintenir un certain de niveau de sécurité, le responsable sécurité ou l'administrateur système, doit au fur et à mesure de leur publication installer les *patches* de sécurité. Si la connaissance des failles et vulnérabilités des systèmes est indispensable au responsable de la sécurité, elle facilite également le travail des malveillants qui peuvent les exploiter avant qu'elles ne soient corrigées. Il est donc impératif de donner les moyens de la réalisation d'une gestion dynamique qui contribue à la mise à jour des solutions de sécurité et au maintien de la sécurité dans le temps.

Si un tel système de publication des correctifs permet encore à l'administrateur de contrôler le processus de mise à jour (acceptation ou non de l'installation des correctifs), un mode automatisé permet de déléguer implicitement à l'éditeur l'installation régulière et systématique des correctifs. Cela pose la question du libre arbitre**.** Quelles sont les conséquences juridiques d'un refus de mise à jour, lors de la survenue de problèmes découlant de l'exploitation d'une faille non corrigée? Etant donné que de nombreuses attaques exploitent ces déficiences, la question du libre arbitre et de la responsabilité de l'administrateur de système est pleinement posée.

---

5 Les points 5.1 et 5.2 sont adaptés de l'article «Sécurité informatique, le piège de la dépendance» A. Dufour, S. Ghernaouti-Hélie, Revue Information et Système, 2006.

La dimension dynamique de la sécurité constitue un défi critique tant pour les fournisseurs de solutions ou éditeurs que pour les administrateurs de systèmes ou responsable sécurité qui ont rarement le temps d'intégrer l'ensemble des correctifs proposés.

La capacité des responsables informatiques ou de la sécurité et des administrateurs système à accéder à toutes les ressources informatiques, implique en plus de l'intégrité sans faille des procédures strictes de surveillance et de contrôle de leurs actions (à la mesure des risques qu'ils font potentiellement courir aux systèmes qu'ils gèrent), leur intégrité morale.

I.2.5.2 Externalisation et dépendance

En proposant des filtres anti-virus ou anti-spam, ces fournisseurs de service gèrent une partie de la sécurité de leurs clients. Si on généralise cette démarche, une évolution de la répartition des rôles et des responsabilités en matière de sécurité est initiée. La sécurité est de plus en plus reportée sur le fournisseur de services ou les intermédiaires techniques. Cette évolution ne résout pas la problématique sécuritaire, elle ne fait que la transférer vers le prestataire de service qui devra non seulement garantir la disponibilité et la performance du service, mais aussi la gestion du maintien de son niveau de sécurité.

En proposant certains logiciels anti-virus, l'éditeur propose également un service de mise à jour automatique. Cette adjonction d'une dimension de service plaide en faveur de la location des logiciels dans la mesure où ceux-ci doivent être maintenus dans la durée par l'éditeur. Elle contribue également à un courant plus global d'externalisation des applications dont le modèle économique est à trouver.

La question de l'externalisation, de la délégation de tout ou partie de la sécurité ne relève pas de la technologie. Elle est de nature stratégique et juridique et pose celle plus fondamentale de la dépendance vis-à-vis de fournisseurs.

La stratégie d'externalisation de la sécurité peut concerner la définition de la politique et sa mise en œuvre, la gestion des accès, de pare-feu (*firewall*), la télémaintenance des systèmes et réseaux, la tierce maintenance applicative, la gestion des sauvegardes, etc. Le choix d'un prestataire doit toujours s'accompagner d'une démarche de contrôle qualité et peut tenir compte, par exemple, de l'expérience du prestataire, des compétences internes, des technologies utilisées, du délai de réaction, du service support, des clauses contractuelles (engagement de résultat, etc.), ou du partage des responsabilités légales.

I.2.5.3 Démarche de prévention et de réaction[6]

La démarche de prévention sécuritaire est par définition pro-active. Elle touche aux dimensions humaine, juridique, organisationnelle, économique (ratio coût de mise en œuvre/niveau de sécurité/services offerts) et technologique. Jusqu'à présent, seule la dimension technologique a été prise majoritairement en considération dans la sécurisation des environnements informatiques. Cette manière d'appréhender la sécurité informatique, sous un angle essentiellement technologique, qui néglige la dimension humaine, pose un véritable problème dans la maîtrise du risque technologique d'origine criminel. En effet, la criminalité est avant tout, une question de personne et non de technologie. Une réponse d'ordre uniquement technologique est donc inappropriée à la maîtrise d'un risque d'origine humaine.

L'appréhension de la criminalité informatique s'inscrit, le plus souvent dans une démarche de réaction et de poursuite. Celle-ci s'effectue à posteriori, c'est-à-dire après la survenue d'un sinistre qui traduit ainsi la défaillance des mesures de protection. Il est nécessaire de prévenir et de dissuader les cyber-abus, en développant des mécanismes de justice et d'investigation, il est tout aussi primordial d'identifier dans les politiques de sécurité, les mesures qui permettront de réagir aux attaques et d'en

---

6 Le point 5.3 est adapté du livre «Sécurité informatique et réseaux» de S. Ghernaouti-Hélie, Dunod 2006.

poursuivre leurs auteurs. Pour cela, il est impératif de concevoir et de réaliser des plans de secours et de continuité qui intègrent les contraintes liées à l'investigation et à la poursuite de la criminalité informatique à des logiques de travail et à des objectifs différents, dans des échelles de temps distinctes.

I.2.6 Point de vue politique

I.2.6.1 Responsabilité de l'Etat

L'état possède des responsabilités importantes pour la réalisation d'une sûreté numérique. Ceci est particulièrement vrai pour la définition d'un cadre légal approprié, c'est-à-dire unifié et applicable. De plus, il doit non seulement favoriser et encourager la recherche et le développement en matière de sécurité mais aussi promouvoir une culture de la sécurité et imposer le respect d'un minimum de normes de sécurité (la sécurité devrait être intégrée en natif dans les produits et services), tout en renforçant la lutte contre la criminalité. Se pose alors la question du modèle financier sous-jacent à ces actions et à la réalisation du partenariat entre le secteur privé et public, pour des plans d'action aux niveaux national et international.

Au niveau stratégique, il faut assurer la prévention, le renseignement, le partage d'information, la gestion des alertes. De plus, il est nécessaire de faire connaître les meilleures pratiques de gestion du risque et de la sécurité. Il est également important d'assurer la coordination et l'harmonisation des systèmes légaux. L'assistance pour promouvoir la sûreté et la sécurité, la définition des coopérations éventuelles (formelle/informelle, multilatérale/bilatérale, active/passive, au niveau national et supra-national, entre autre, sont aussi à définir.

Il également essentiel d'éduquer, d'informer et former aux technologies de traitement de l'information et des communications et non uniquement à la sécurité et aux mesures de dissuasion. La sensibilisation aux problématiques de sécurité ne doit pas se limiter à la promotion d'une certaine culture de la sécurité et d'une cyberéthique. En amont de la culture sécuritaire, il doit y avoir une culture de l'informatique.

Il faut donner les moyens aux différents acteurs d'apprendre à gérer les risques technologique, opérationnel et informationnel qui les menacent en fonction de l'usage fait des nouvelles technologies. Dans ce contexte, l'Etat doit aussi favoriser le signalement des agressions liées au cybercrime et instaurer la confiance entre les différents acteurs du monde économiques et les services de justice et de police.

Services de justice et police mais aussi ceux de la protection civile, les pompiers, l'armée ou la Gendarmerie trouvent leur place tant au niveau tactique qu'opérationnel dans la lutte contre la criminalité informatique afin de protéger, poursuivre et réparer. Des centres de surveillance, de détection et d'information aux risques informatique et criminel doivent être opérationnels afin d'assurer la prévention nécessaire à la maîtrise de ces risques.

Il est de la responsabilité des Etats de définir une véritable politique de développement de la société de l'information en fonction de ses valeurs propres et de mettre à disposition les moyens nécessaires pour cette réalisation. Cela concerne également les moyens de protection et de lutte contre la cybercriminalité.

Une maîtrise globale, centralisée et coordonnée de la criminalité informatique nécessite une réponse politique, économique, juridique et technologique homogène et adoptable par les différents acteurs de la chaîne numérique, co-partenaires de la sécurité.

I.2.6.2 Souveraineté des Etats

Le défi de la simplicité et de l'efficacité de la sécurité s'oppose à la complexité des besoins et des environnements, tend à favoriser les démarches d'externalisation des services et de la sécurité des systèmes et des informations à de sociétés spécialisées. Cette externalisation induit une dépendance

forte, quand elle n'est pas totale. Cela constitue un risque sécuritaire majeur. Les Etats doivent être attentifs à ne pas être dépendant pour leur gestion stratégique, tactique et opérationnelle de leur sécurité, d'entités externes qu'ils ne peuvent contrôler.

Les Etats doivent contribuer à imposer:

- de pouvoir disposer de la sécurité en mode natif (sécurité par défaut) et de manière conviviale, compréhensible, transparente, contrôlable et vérifiable;
- d'éviter que les individus et Institutions se mettent en situations dangereuses (éviter les configurations permissives, les comportement à risques, la dépendance excessive, etc.);
- le respect des normes de sécurité;
- une réduction des vulnérabilités dans les technologies et dans les solutions de sécurité.

I.2.7 Point de vue économique

La sécurité ne permet pas directement de gagner de l'argent mais évite d'en perdre. S'il peut paraître relativement aisé d'estimer ce que coûte la sécurité (budgets associés, coût des produits de sécurité, des formations, etc.), il est plus délicat d'évaluer la rentabilité de la sécurité. De manière subjective, on peut penser que les mesures de sécurité possèdent intrinsèquement une efficacité «passive» et évitent certaines pertes.

Toutefois, déterminer le coût de la sécurité en regard des coûts engendrés par les conséquences résultants de la perte de valeurs suite à des accidents, erreurs ou à de la malveillance est difficile à réaliser. Le coût de la sécurité est fonction des exigences des organisations et dépend des valeurs à protéger, du coût des préjudices consécutifs à un défaut de sécurité. Aussi, il n'existe pas de réponse prédéfinie aux questions suivantes:

- Comment évaluer l'exposition de l'organisation aux risques, notamment aux risques sériels dus à l'interconnexion des infrastructures inter-organisations?
- Comment estimer correctement les coûts indirects de l'insécurité, résultant par exemple d'une perte d'image ou de l'espionnage?
- Que peut rapporter la sécurité pour l'organisation qui la met en œuvre?
- Quelle est la valeur économique de la sécurité?
- Quel est le retour sur investissement de la sécurité?

La valeur économique de la sécurité est à appréhender dans toute sa dimension sociétale et tient compte des impacts des nouvelles technologies pour les individus, les organisations et les nations. Elle ne peut se réduire à des coûts d'installation et de maintenance.

I.2.8 Point de vue social

Il est important de sensibiliser l'ensemble des acteurs du monde de l'internet aux enjeux de la maîtrise de la sécurité et aux mesures élémentaires qui si elles sont clairement énoncées, définies et mise en œuvre intelligemment, renforceront le niveau de sécurité.

Des actions d'information et d'éducation civique à une société de l'information responsable, sur les enjeux, les risques et les mesures préventives et dissuasives de sécurité sont nécessaires pour éduquer l'ensemble des cybercitoyens à adopter une démarche sécurité.

L'accent sera mis sur le devoir de sécurité, sur la responsabilité individuelle et sur les mesures dissuasives, ainsi que les conséquences pénales potentielles résultant du non-respect des obligations sécuritaires. De manière plus générale, il est également nécessaire d'éduquer et de former aux technologies de traitement de l'information et des communications et non uniquement à la sécurité et aux mesures de dissuasion. La sensibilisation aux problématiques de sécurité ne doit pas se limiter à la

promotion d'une certaine culture de la sécurité. En amont de la culture sécuritaire, il doit y avoir une culture de l'informatique ce qui correspond à la notion de permis de conduire informatique, que prône le CIGREF (Club Informatique des Grandes Entreprises Française)[7].

Faisons de l'internet un patrimoine ouvert à chacun de sorte que les cybercitoyens puissent potentiellement bénéficier des infrastructures et services mis à leur disposition, sans pour autant prendre des risques sécuritaires excessifs. Une éthique sécuritaire doit donc être développée, comprise et respectée par tous les acteurs du cyberespace.

I.2.9 Point de vue juridique

I.2.9.1 Facteur critique de succès

Certaines législations nationales ou conventions internationales contraignent les organisations à se doter de mesures de sécurité leur assurant la conformité juridique. Ainsi les dirigeants d'une organisation et par le biais de la délégation de pouvoir, les responsables de sécurité ont une obligation de moyens de la sécurité (mais non une obligation de résultat). La responsabilité d'une personne morale mise en défaut de sécurité lors d'une infraction établie peut être pénale, civile ou administrative. Cette responsabilité est établie sans préjudice de la responsabilité pénale des personnes physiques ayant commis l'infraction.

Une législation adaptée en matière de traitement des données permet de renforcer la confiance des partenaires économiques envers les infrastructures d'un pays. Cela participera au développement économique de celui-ci. Ainsi, en contribuant à réaliser un contexte propice à l'échange de données basé sur le respect des législations, ces dernières favorisent l'adoption par le grand public de services basés sur l'informatique et les télécommunications. La législation et la sécurité, sont alors à considérer comme des leviers de l'économie nationale. Associées aux notions de confiance et de qualité, la cbersécurité constituent les pierres angulaires qui permettent de développer une véritable économie de services.

I.2.9.2 Renforcer la législation et les moyens de l'appliquer

A l'heure actuelle, la cybercriminalité est mal maîtrisée comme continu de le démontrer les chiffres des sondages annuels du CSI[8] (*Computer Security Institute*) ou les statistiques du CERT[9] (*Computer Emergency and Response Team*). Ainsi, il est constaté que les mesures de sécurité mises en place par les institutions tendent à protéger un environnement donné dans un contexte particulier, mais ne peuvent aucunement empêcher la conduite d'activités criminelles via l'internet. Les raisons de cette situation sont notamment liées:

- aux caractéristiques du cybercrime (capacité à être automatisé, savoir-faire embarqué dans le logiciel, réalisation à distance);
- à la possibilité offerte au cybercriminel d'usurper facilement et sans risque excessif, l'identité d'utilisateurs légitimes, ruinant par là même la capacité de la justice à identifier les auteurs réels d'une infraction;
- à la détermination des compétences pour réaliser une enquête;
- à la pénurie de ressources humaines et matérielles au sein des services chargés de la répression – des crimes et délits informatiques;
- au caractère transnational de la cybercriminalité qui nécessite des recours fréquents à la coopération et à l'entraide judiciaire internationale. Cette dernière implique des contraintes de temps non compatibles avec la rapidité d'exécution des agressions et les besoins de reprise immédiate des systèmes informatiques concernés par les cyberattaques;

---

7 CIGREF: www.cigref.fr.

8 CSI: www.gocsi.com

9 CERT: www.cert.org

– à la difficulté de qualifier les faits au regard de certaines législations pénales;
– à la nature mal définie et à la volatilité de la plupart des preuves informatiques.

Pour toutes ces causes, le système judiciaire dans le contexte de l'internet, n'est pas efficace. De plus, de même qu'il existe des paradis fiscaux, il existe des paradis légaux. Ce n'est pas nécessairement par absence de lois, que le crime informatique est peu ou mal réprimé. Un certain nombre de crimes et de délits informatiques sont déjà qualifiés par le biais des législations pénales existantes.

Ce qui est illégal «off-line» est illégal «on-line»

De nouvelles législations, nées de la nécessité de définir un cadre juridique approprié à l'usage des nouvelles technologies, complètent ou doivent compléter la plus part des législations existantes qui sont, rappelons-le, également valides dans le cyberespace.

Renforcer la législation n'est pas forcément suffisant, si les moyens de l'appliquer manquent. Une loi est de peu d'utilité, si la justice n'est pas en mesure de collecter et de traiter les preuves, d'identifier et de sanctionner les auteurs de comportements criminels. Elle n'est pas efficace si les malveillants ont le sentiment d'agir en toute impunité.

I.2.9.3 Lutte contre la cybercriminalité et droit à l'intimité numérique: un compromis difficile

Les moyens de lutte contre le fléau grandissant et transfrontalier qu'est la cybercriminalité passe par la mise à disposition d'un cadre légal harmonisé au niveau international et applicable et des moyens d'une véritable coopération internationale des instances de justice et police.

L'Etat possède des responsabilités importantes pour la réalisation d'une sûreté numérique. Ceci est particulièrement vrai pour la définition d'un cadre légal approprié, c'est-à-dire unifié et applicable, pour la promotion d'une culture de la sécurité qui respecte l'intimité numérique des individus (*privacy*), tout en renforçant la lutte contre la criminalité.

La lutte contre la cybercriminalité doit avoir comme objectif principal la protection des individus, des organisations et des Etats, en tenant compte des grands principes démocratiques.

Les outils de lutte contre la criminalité informatique peuvent potentiellement mettre à mal les droits de l'homme et aller à l'encontre de la confidentialité des données à caractère personnel. En effet, la sécuriser passe par la surveillance, le contrôle et le filtrage des données. Il est impératif que des gardes fous soient mis en place pour éviter des abus de pouvoir, de situation dominante et toute sorte de dérives totalitaires afin de garantir le respects des droits fondamentaux, notamment celui du respect de l'intimité numérique et de la confidentialité des données personnelles.

Outre la directive européenne de 1995, remarquons que diverses législations nationales existent depuis déjà longtemps concernant la protection des données personnelles:

Allemagne:	loi du 21 janvier 1977
Argentine:	loi sur la protection des données personnelles – 1996
Autriche:	loi du 18 octobre 1978
Australie:	loi sur la vie privée – 1978
Belgique:	loi du 8 décembre 1992
Canada:	loi sur la protection des renseignements personnels – 1982
Danemark:	loi du 8 juin 1978
Espagne:	loi du 29 octobre 1992
Etats-Unis:	loi sur la protection des libertés individuelles – 1974; loi sur les bases de données et la vie privée – 1988
Finlande:	loi du 30 avril 1987
France:	loi informatique et liberté du 6 janvier 1978 – modifiée en 2004
Grèce:	loi du 26 mars 1997
Hongrie:	loi sur la protection des données personnelles et la communication des données publiques – 1992

Irlande:	loi du 13 juillet 1988
Islande:	loi relative à l'enregistrement des données personnelles – 1981
Israël:	loi sur la protection de la vie privée – 1981, 1985, 1996; Loi sur la protection des données dans l'administration – 1986
Italie:	loi du 31 décembre 1996
Japon:	loi sur la protection des données informatisées à caractère personnel – 1988
Luxembourg:	loi du 31 mars 1979
Norvège:	loi sur les registres des données personnelles – 1978
Nouvelle-Zélande:	loi sur l'information officielle – 1982
Pays-Bas:	loi du 28 décembre 1988
Pologne:	loi relative à la protection des données personnelles – 1997
Portugal:	loi du 29 avril 1991
République tchèque:	loi sur la protection des données personnelles des systèmes informatisés – 1995
Royaume-Uni:	loi du 12 juillet 1988
Russie:	loi fédérale sur l'information, l'informatisation et la protection des informations
Slovénie:	loi sur la protection des données – 1990
Suède:	11 mai 1973
Suisse:	loi fédérale sur la protection des données – 1992
Taiwan:	loi sur la protection des données – 1995

I.2.9.4 Réglementation internationale en matière de cybercriminalité

La première réglementation internationale, contribuant à appréhender la dimension internationale de la cyber criminalité est la Convention sur la cybercriminalité[10] – Budapest 23 novembre 2001, adoptée sous l'égide du Conseil de l'Europe et entrée en vigueur en juillet 2004 (dès sa ratification par au moins 5 Etats (dont 3 au moins être doivent du Conseil de l'Europe). Cette convention aborde les points suivants:

- Disposition de droit pénal matériel concernant:
  - les infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques;
  - les infractions informatiques;
  - les infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes;
- Disposition de droit procédural concernant:
  - la conservation rapide des données informatiques, de données relatives au trafic et à sa divulgation rapide à l'autorité compétente;
  - la conservation et la protection de l'intégrité des données pendant une durée aussi longue que nécessaire pour permettre aux autorités compétentes d'obtenir leur divulgation;
  - l'injonction de produire;
  - la perquisition et la saisie des données stockées;
  - la collecte en temps réel des données;
  - la protection adéquate des droits de l'homme et des libertés;
- Chaque Etat doit adopter des mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, dans le respect de son droit interne:
  - l'accès intentionnel et sans droit à tout ou partie d'un système;
  - l'interception intentionnelle et sans droit de données lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système;

[10] www.conventions.coe.int/Treaty/FR/Treaties/Html/185.htm

- le fait intentionnel et sans droit d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données;
- l'entrave grave intentionnelle et sans droit au fonctionnement d'un système;
- la production, la vente, l'obtention pour l'utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition d'un dispositif conçu ou adapté pour réaliser une des infractions mentionnées;
- l'introduction, l'altération, l'effacement ou la suppression intentionnelle et sans droit de données, engendrant des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales, comme si elles étaient authentiques;
- le fait intentionnel et sans droit de causer un préjudice patrimonial à autrui par l'introduction, l'altération, l'effacement ou la suppression de données, toute forme d'atteinte au fonctionnement d'un système, dans l'intention frauduleuse ou délictueuse, d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui;
- la complicité en vue …est érigée en infraction pénale ainsi que la tentative intentionnelle de …

– Les Etats doivent établir leurs compétences à l'égard de toute infraction pénale lorsque cette dernière est commise:
  - sur son territoire;
  - à bord d'un navire battant pavillon de cet Etat;
  - par un de ses ressortissants, si l'infraction est punissable pénalement là ou elle a été commise ou si l'infraction ne relève pas de la compétence territoriale d'aucun Etat;
– Règles concernant la coopération internationale en matière:
  - d'extradition;
  - d'entraide aux fins d'investigation;
  - de procédures concernant les infractions pénales liées à des systèmes et données informatiques;
  - de recueil de preuves sous forme électronique d'une infraction pénale;
– Création d'un réseau d'entraide
  - 24h/24, 7j/7;
  - point de contact national;
  - assistance immédiate pour les infractions;

Une volonté réglementaire existe bien au niveau international de pouvoir maîtriser la cybercriminalité. Ce n'est pas toujours par absence de Lois, ou de principes directeurs comme ceux énoncés par l'OCDE (Organisation de coopération et de développement économiques) «Lignes directrices de l'OCDE régissant la sécurité des systèmes et des réseaux – vers une culture de la sécurité – 2002[11]» (Figure I.7) mais ce sont la difficulté et la complexité du chantier à mettre en œuvre et les moyens nécessaires pour atteindre les objectifs de lutte contre non seulement la cybercrimnalité mais aussi le crime organisé, qui font que l'internet est exploité à des fins malveillantes.

---

[11] www.oecd.org/dataoecd/16/22/15582260.pdf. Les directives sont rappelées en annexe de ce document.

Figure I.7 – Lignes directrices de l'OCDE en matière de sécurité informatique (juillet 2002)

Sensibilisation	Les parties prenantes doivent être sensibilisées au besoin d'assurer la sécurité des systèmes et des réseaux d'information et aux actions qu'elles peuvent entreprendre pour renforcer la sécurité
Responsabilité	Les parties prenantes sont responsables de la sécurité des systèmes et des réseaux d'information
Réaction	Les parties prenantes doivent agir avec promptitude et dans un esprit de coopération pour prévenir, détecter et répondre aux incidents de sécurité
Ethique	Les parties prenantes doivent respecter les intérêts légitimes des autres parties prenantes
Démocratie	La sécurité des systèmes et des réseaux d'information doit être compatible avec les valeurs fondamentales d'une société démocratique
Evaluation des risques	Les parties prenantes doivent procéder à des évaluations des risques
Conception et mise en oeuvre de la sécurité	Les parties prenantes doivent intégrer la sécurité en tant qu'un élément essentiel des systèmes et réseaux d'information
Gestion de la sécurité	Les parties prenantes doivent adopter une approche globale de la gestion de la sécurité
Réévaluation	Les parties prenantes doivent examiner et réévaluer les sécurité des systèmes et réseaux d'information et introduire les modifications appropriées dans leur politique, pratiques, mesures et procédures d sécurité

I.2.10 Fondamentaux de la cybersécurité

Les solutions de sécurité doivent contribuer à satisfaire les critères de base de la sécurité que sont la disponibilité, l'intégrité et la confidentialité (critères DIC). A ces trois premiers critères s'ajoutent ceux qui permettent de prouver l'identité des entités (notion d'authentification) et que des actions ou évènements ont bien eu lieu (notions de non répudiation, d'imputabilité voire de traçabilité) (Figure I.8).

I.2.10.1 Disponibilité

La disponibilité des services, systèmes et données est obtenue, d'une part, par un dimensionnement approprié et une certaine redondance des éléments constitutifs des infrastructures et, d'autre part, par une gestion opérationnelle des ressources et des services.

La disponibilité est mesurée sur la période de temps pendant laquelle le service offert est opérationnel. Le volume potentiel de travail susceptible d'être pris en charge durant la période de disponibilité d'un service, détermine la capacité d'une ressource (serveur ou réseau par exemple). La disponibilité d'une ressource est, en outre, indissociable de son accessibilité.

I.2.10.2 Intégrité

Le respect de l'intégrité des données, traitements ou services permet d'assurer qu'ils ne sont pas modifiés, altérés ou détruits tant de façon intentionnelle qu'accidentelle. Cela contribue à assurer leur exactitude, leur fiabilité et leur pérennité.

Il convient de se prémunir contre l'altération des données en ayant la certitude qu'elles n'ont pas été modifiées lors de leur stockage ou de leur transfert.

L'intégrité des données ne sera garantie que si elles sont protégées des écoutes actives qui peuvent modifier les données interceptées. Cette protection pourra être réalisée par la mise en œuvre de mécanismes de sécurité tels que:

– un contrôle d'accès rigoureux;
– un chiffrement des données;
– des moyens de protection contre les virus, les vers ou les chevaux de Troie.

Figure I.8 – Fondamentaux de la cybersécurité

Capacité d'un système à:	Objectifs de sécurité	Moyens de sécurité
Pouvoir être utilisé	▪ Disponibilité ▪ Pérennité ▪ Continuité ▪ Confiance	▪ Dimensionnement ▪ Redondance ▪ Procédures d'exploitation et de sauvegarde
Exécuter des actions	▪ Sureté de fonctionnement ▪ Fiabilité ▪ Durabilité ▪ Continuité ▪ Exactitude	▪ Conception ▪ Performances ▪ Ergonomie ▪ Qualité de service ▪ Maintenance opérationnelle
Permettre l'accès aux entités autorisées (aucun accès illicite)	▪ Confidentialité (maintien du secret) ▪ Intégrité (aucune modification)	▪ Contrôle d'accès ▪ Authentification ▪ Contrôle d'erreur ▪ Contrôle de cohérence ▪ Chiffrement
Prouver des actions	▪ Non-répudiation ▪ Authenticité (aucun doute) ▪ Aucune contestation	▪ Certification ▪ Enregistrement, traçabilité ▪ Signature électronique ▪ Mécanismes de preuve

I.2.10.3 Confidentialité

La confidentialité est le maintien du secret des informations, des flux, des transactions, services ou actions réalisées dans le cyberespace. Il s'agit de la protection des ressources contre une divulgation non autorisée.

La confidentialité peut être réalisée par la mise en œuvre de mécanismes de contrôle d'accès ou de chiffrement.

Le chiffrement des données (ou cryptographie), contribue à assurer la confidentialité des informations lors de leur transmission ou de leur stockage en les transformant de façon à ce qu'elles deviennent inintelligibles aux personnes ne possédant pas les moyens de les déchiffrer.

I.2.10.4 Identification et authentification

L'authentification doit permettre de ne pas avoir de doute sur l'identité d'une ressource. Cela suppose que toutes les entités (ressources matérielles, logicielles ou personnes) soient correctement identifiées et que certaines caractéristiques puissent servir de preuve à leur identification. Tous les mécanismes de contrôle d'accès logique aux ressources informatiques nécessitent notamment de gérer l'identification et l'authentification des entités.

Les processus d'identification et d'authentification sont mis en œuvre pour contribuer à réaliser:

- la confidentialité et l'intégrité des données (seuls les ayant droits identifiés et authentifiés peuvent accéder aux ressources (contrôle d'accès et les modifier s'ils sont habilités à le faire);
- la non répudiation et l'imputabilité (les entités identifiées et authentifiées ont réalisées telle action), la preuve de l'origine d'un message, d'une transaction (une entité identifiée et authentifiée à effectuée une émission), la preuve de la destination (une entité identifiée et authentifiée est destinatrice d'un message).

I.2.10.5 Non répudiation

Dans certaines circonstances, il est nécessaire de prouver la réalisation de certains évènements (action, transaction). A la non-répudiation sont associés les notions de responsabilité d'imputabilité, de traçabilité et éventuellement d'auditabilité.

L'établissement de la responsabilité nécessite l'existence de mécanismes d'authentification des individus et d'imputabilité de leurs actions. Le fait de pouvoir enregistrer des informations afin de pouvoir «tracer» la réalisation d'actions est important lorsqu'il s'agit de reconstituer un historique des évènements, notamment lors d'investigations en milieu informatique pour retrouver éventuellement l'adresse d'un système à partir de laquelle des données ont été envoyées par exemple. Les informations nécessaires à une analyse ultérieure (journalisation des informations) permettant l'audit d'un système doivent être sauvegardées. Cela constitue la capacité des systèmes à être audités (notion d'auditabilité).

I.2.10.6 Sécurité physique

Les environnements qui abritent les postes de travail, les serveurs, les zones d'exploitation informatique et de logistique (air conditionné, tableaux de contrôle de l'alimentation électrique, etc.) doivent être physiquement protégés contre des accès indus et des catastrophes naturelles (feu, inondation, etc.). La sécurité physique représente le contrôle le plus fondamental et le plus courant des systèmes informatiques.

I.2.10.7 Solutions de sécurité

A la vue des problèmes sécuritaires qui constituent la réalité quotidienne de la plus part des infrastructures, constatant que les solutions de sécurité ne manquent pas, et que le marché de la sécurité se porte plutôt bien, nous sommes en droit de nous poser les questions suivantes:

- les solutions de sécurité sont-elles adaptées aux besoins?
- sont-elles implantées et gérées correctement?
- peuvent-elles s'appliquer, s'adapter à un environnement en perpétuelle mutation?
- peuvent-elles pallier le pouvoir excessif accordé aux administrateurs systèmes?
- comment peuvent-elles faire face aux problèmes sécuritaires dont l'origine est à rechercher dans la négligence, l'incompétence, les défaillances lors de la conception, de la mise en œuvre ou de la gestion des technologies et des solutions de sécurité?
- etc.

SECTION II

MAÎTRISE DE LA CYBERCRIMINALITÉ

Chapitre II.1 – Cybercriminalité

II.1.1 Notions de crime informatique et de cybercrime

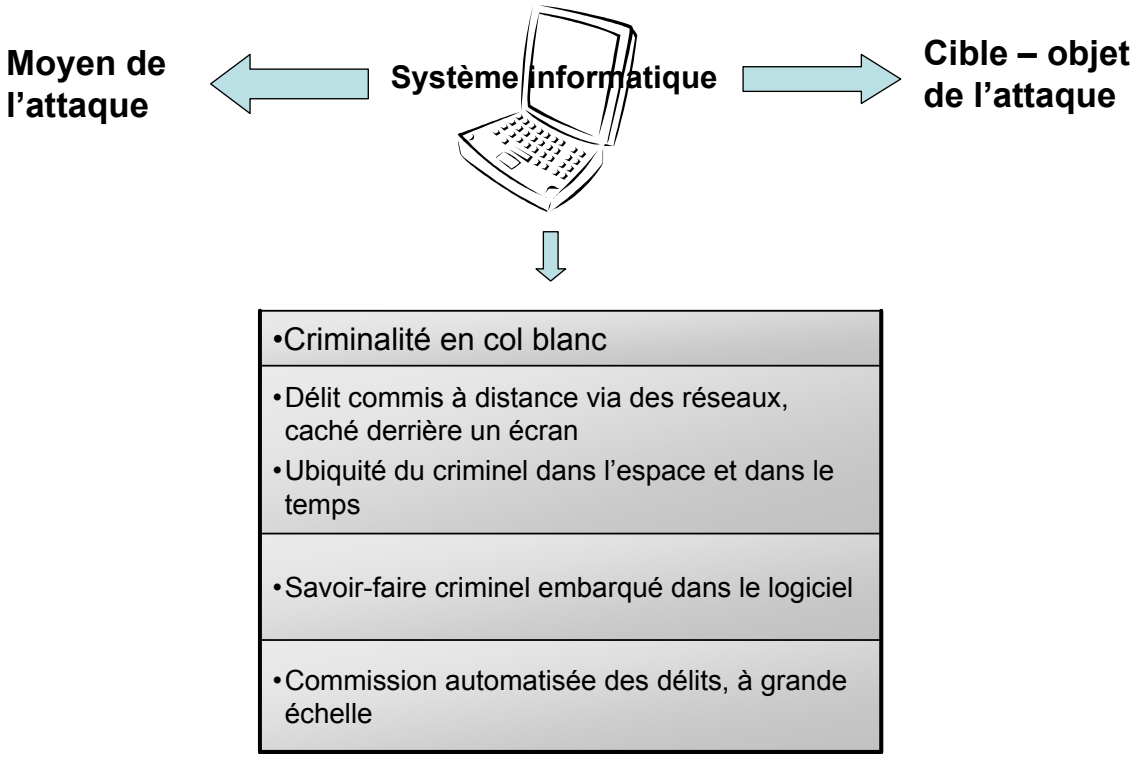
Les vulnérabilités et la maîtrise insuffisante des technologies du numérique leur confèrent un certain niveau d'insécurité. Cet état d'insécurité est largement exploité par les acteurs du monde criminel. De plus, chaque technologie est porteuse de potentialités criminelles et offre des opportunités pour réaliser des infractions. L'internet n'échappe pas à cette règle et le monde criminel a investi le cyberespace.

L'OCDE a défini en 1983 l'infraction informatique comme étant tout comportement illégal, immoral ou non autorisé qui implique la transmission et/ou le traitement automatique de données.

Un crime informatique (*computer-related crime*) est un délit pour lequel un système informatique est l'objet du délit et/ou le moyen de le réaliser, c'est un crime lié aux technologies du numérique qui fait partie de la criminalité en col blanc. Le cybercrime (*cybercrime*) est une forme du crime informatique qui fait appel aux technologies de l'internet pour sa réalisation. Cela concerne tous les délits réalisés dans le cyberespace.

Le monde virtuel confère au crime la capacité à être automatisé, autorisant une réalisation à grande échelle (cyberépidémie), permettant d'être commis à distance *via* les réseaux (ubiquité du criminel, dans le temps et dans l'espace) et avec éventuellement des effets à retardement (Figure II.1).

Figure II.1 – Caractéristiques du crime informatique



Les technologies de l'internet facilitent toute sorte d'infractions (vol, sabotage d'informations, atteintes au copyright, au droit d'auteur, à la violation du secret professionnel, de l'intimité numérique, de la propriété intellectuelle, dissémination de contenus illégaux, attaques concurrentielles, espionnage industriel, atteinte aux droits des marques, diffusion de fausses informations, dénis de service, fraudes diverses, etc.).

Les évènements qui ont contribué à l'évolution de la perception de la menace cybercriminelle sont outre le bug de l'an 2000 qui a fait prendre conscience de la fragilité des logiciels et de la dépendance vis-à-vis de l'informatique, sont les attaques de déni de service contre des sites tels que Yahoo (10 février 2000) et le fameux virus «I love you» (du 4 mai 2000). Depuis, associé à la médiatisation d'infections virales (virus *Code red* juillet 2001 ou *Nimda* septembre 2001) ou de dénis de services (attaque des principaux serveurs DNS 21 octobre 2002) pour ne citer que quelques exemples, le grand public prend plus ou moins conscience de la réalité des menaces s'effectuant à travers le monde de l'internet. L'actualité reste riche en nouvelles de révélation de problèmes liés à l'informatique.

II.1.2 Facteurs qui favorisent l'expression de la criminalité via l'internet

II.1.2.1 Monde virtuel et dématérialisation

La dématérialisation des transactions, les facilités de communication associées aux solutions de chiffrement, de stéganographie et d'anonymat, autorisent des liaisons entre criminels de différents pays sans contact physique, de manière flexible et sécurisée en toute impunité. Ainsi, ils peuvent s'organiser en équipes, planifier des actions illicites et les réaliser soit de manière classique, soit par le biais des nouvelles technologies. La couverture internationale du réseau internet permet aux criminels d'agir au niveau mondial, à grande échelle et très rapidement.

Outre, ces facilités inhérentes au monde numérique et aux télécommunications, les problèmes de conception, de mise en œuvre, de gestion, et de contrôle de l'informatique, associés aux pannes, aux dysfonctionnements, aux erreurs, aux incompétences, ou encore aux catastrophes naturelles, comme l'interdépendance des infrastructures, confèrent de facto un certain niveau d'insécurité aux infrastructures numériques.

Les possibilités d'exploitation des vulnérabilités à des fins malveillantes sont nombreuses.

La réalité de ces dernières:

> usurpation d'identité, leurre, accès indus, exploitation frauduleuse de ressources, infection, détérioration, destruction, modification, divulgation, vol de données, chantage, extorsion, racket, déni de service, etc.

met en évidence une maîtrise insuffisante du risque informatique d'origine criminelle par les organisations et les limites des approches sécuritaires actuelles.

Le cyberespace, où les actions se réalisent cachées derrière un écran et à distance à travers un réseau, favorise les comportements criminels. Cela facilite pour certains, le passage à l'illégalité sans parfois de prise de conscience réelle de la dimension criminelle des actes perpétrés.

De plus, les criminels peuvent s'organiser en équipes, planifier des actions illicites et les réaliser soit de manière classique, soit par le biais des nouvelles technologies. La couverture internationale du réseau internet permet aux criminels d'agir au niveau mondial, à grande échelle et très rapidement.

II.1.2.2 Mise en réseau des ressources

La généralisation de la mise en réseau des ressources informatiques et informationnelles, font qu'elles deviennent des cibles attrayantes pour la réalisation de crimes économiques via les nouvelles technologies. Les différentes formes d'attaques informatiques existantes ont pour dénominateur commun qu'elles font courir relativement peu de risques à leur auteur et possèdent des conséquences négatives et dommages potentiels bien supérieurs aux ressources nécessaires pour les réaliser. L'usurpation d'identité électronique, les possibilités d'anonymat ou la prise de contrôle d'ordinateurs par exemple, facilitent la réalisation d'actions illégales sans prise de risque excessive.

II.1.2.3 Disponibilité d'outils et existence de failles

La disponibilité d'outils d'exploitation des failles et vulnérabilité des systèmes, de bibliothèques d'attaques et de logiciels qui capitalisent le savoir-faire criminel dans un programme, facilite la réalisation des attaques informatiques. Cette disponibilité associée à la dématérialisation des actions, favorise le comportement malveillant des informaticiens qui possèdent la fibre criminelle et des criminels qui possèdent des aptitudes en informatique. Le cyberespace facilite pour certains, le passage à l'illégalité sans parfois de prise de conscience réelle de la dimension criminelle des actes perpétrés.

II.1.2.4 Vulnérabilité et défaillance

La criminalité tire partie des vulnérabilités et défaillances organisationnelles et techniques de l'internet, de l'absence d'un cadre juridique harmonisé entre les Etats et d'un manque de coordination efficace des polices. Il peut s'agir de criminalité classique (commission de vieux délits avec de nouvelles technologies: blanchiment d'argent, chantage, extorsion, etc.) ou générer de nouveaux types de délits à partir des technologies du numérique: intrusion dans des systèmes, vol de temps processeur, vol de code source, de bases de données, etc. Dans tous les cas, ils s'effectuent dans des conditions exceptionnelles d'optimalité (risques minimaux, couverture importante, profitabilité maximale).

La Figure II.2 rappelle les sources de vulnérabilités d'une infrastructure internet.

Figure II.2 – Principales caractéristiques du monde de l'internet exploitées à des fins criminelles

II.1.2.5 Difficulté à identifier l'auteur d'un délit

Le crime informatique est un crime sophistiqué, réalisé le plus souvent au niveau international avec parfois un effet à retardement. Les traces laissées dans les systèmes sont immatérielles et difficiles à collecter et à sauvegarder. Il s'agit d'informations numériques mémorisées sur toute sorte de supports: mémoire, périphériques de stockage, disque dur, disquettes, clé USB, divers composants électroniques, etc. Il se pose alors la question de leurs saisies lors d'une perquisition informatique. Les questions suivantes entre autres, montrent à quel point la notion de preuve numérique est difficile à établir:

- comment identifier les données pertinentes?
- comment les localiser?
- comment les sauvegarder?
- comment constituer une preuve recevable auprès d'un tribunal?
- comment récupérer des fichiers effacés?
- comment prouver l'origine d'un message?
- comment remonter jusqu'à l'identité d'une personne sur la base uniquement d'une trace numérique du fait qu'il est difficile d'établir une correspondance certaine entre une information numérique et son auteur (dématérialisation) et de l'usurpation d'identité fréquente?
- quelle est la valeur d'une trace numérique en tant que preuve contribuant à établir la vérité auprès d'un tribunal (notion de preuve numérique) sachant que les supports de mémorisation sur lesquelles des traces ont été recueillies sont faillibles (les notions de date et d'heure sont variables d'un système informatique à l'autre et aisément modifiables).
- etc.

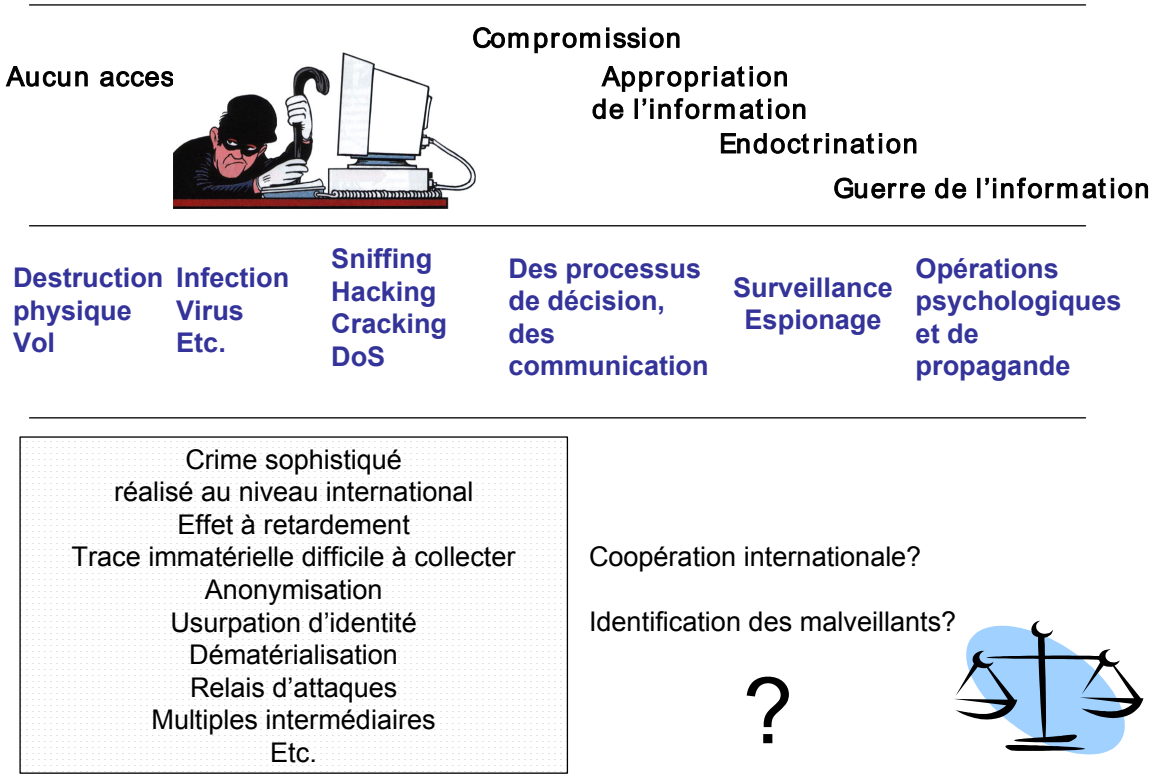
Les traces informatiques sont d'autant plus difficiles à obtenir lorsqu'elles sont laissées dans des systèmes ressortissants de différents pays. Leur obtention relève de l'efficacité de l'entraide judiciaire internationale et de la rapidité d'intervention. Leur exploitation efficace pour identifier des individus dépend de la durée de traitement de la requête d'obtention qui peut mettre un certain temps et qui rend alors toute identification impossible.

La Figure II.3 identifie différents types de problèmes induits par la malveillance comme la destruction physique ou le vol de matériel qui empêche l'accès aux systèmes et données, comme l'infection des ressources, la compromission des processus de décision ou de communication par des attaques de déni de service (ou suite à de l'espionnage ou à l'intrusion dans des systèmes), l'appropriation illégale ou la manipulation d'informations (endoctrination, guerre de l'information). Elle met également en évidence les principales caractéristiques du cybercrime qui rendent difficiles l'identification des malveillants.

Par ailleurs, dans la plupart des Etats, il existe un décalage significatif entre les aptitudes des criminels à effectuer des crimes de haute technologie et les moyens mis à disposition des forces de justice et police pour les poursuivre. Le niveau d'adoption des nouvelles technologies par les instances de justice et de police aux niveaux national et international reste faible et très disparate d'un pays à l'autre.

Ce sont généralement les moyens courants d'investigation des crimes conventionnels auxquels ont recours les forces de justice et police pour poursuivre les cybercriminels qui permettent de les identifier et de les arrêter.

Figure II.3 – Difficulté à identifier un malveillant



II.1.2.6 Aterritorialité et paradis numériques

Le monde criminel tire partie de l'aterritorialité de l'internet, de l'inexistence dans certains Etats de lois réprimant le crime informatique et des juridictions multiples dont relève l'internet

De manière analogue aux paradis fiscaux des paradis numériques permettent aux criminels d'héberger des serveurs, diffuser des contenus illicites ou réaliser des actions illicites en toute impunité. Le fait de pouvoir localiser des serveurs dans des Etats faibles constituent des refuges à des opérations transnationales.

Le manque de régulation internationale et de contrôle, l'inefficacité de la coopération internationale en matière d'investigation et de poursuites judiciaires font que l'internet offre une couche d'isolation protectrice aux criminels.

A l'heure actuelle, aucune réponse correcte tant sur le plan juridique que technique est apportée pour maîtriser les différents délits favorisés par l'internet tels que:

- l'industrie parallèle et très organisée de la copie à la chaîne de logiciels, de films, de musique, etc., qui a pris dans le cyberespace une dimension sans précédent;
- les atteintes au copyright, droits d'auteur, la violation du secret professionnel, de l'intimité numérique ou de la propriété intellectuelle;
- les atteintes à la propriété, l'appropriation illégale de la propriété d'autrui, l'endommagement, la destruction de la propriété d'autrui ou l'immixtion dans la propriété d'autrui (notion de violation de domicile virtuel);
- la dissémination de contenus illégaux;
- attaques concurrentielles, espionnage industriel, atteinte aux droits des marques, diffusion de fausses informations, dénis de service commandités par des concurrents.

II.1.3 Criminalité classique et cybercriminalité

La cybercriminalité constitue le prolongement naturel de l'expression de la criminalité classique. De nos jours, les activités criminelles s'effectuent à travers le cyberespace, par d'autres moyens que ceux habituellement mis en œuvre, et de manière complémentaire à la criminalité classique.

Non seulement l'internet offre des conditions exceptionnelles pour de nouvelles entreprises et activités illicites, mais il autorise également la réalisation de fraudes ou délits habituels via l'outil informatique.

L'internet offre des opportunités pour favoriser la recherche et la production de revenus, De ce fait, il accorde de nouvelles capacités au monde criminel. Une exploitation efficace des nouvelles technologies, permet aux criminels de réaliser des délits tout en assurant la maximisation des bénéfices et en exposant à un niveau de risque acceptable pour les criminels.

II.1.4 Cybercriminalité, criminalité économique et blanchiment

Le crime économique via l'internet n'est pas uniquement réservé à la criminalité organisée, les outils informatiques et télécoms le mettent à la portée d'individus isolés, qui peuvent se constituer ou non, en groupes plus ou moins importants.

Les criminels peuvent s'organiser autour de l'échange d'informations grâce aux technologies de l'information. Des réseaux de personnes ou de compétences autorisent la constitution d'organisations criminelles dématérialisées.

Le haut degré de compétence économique et le professionnalisme nécessaire à la réalisation du crime économique, font que celui-ci peut être facilité par les technologies de l'information.

L'internet contribue à l'acquisition des informations, à une meilleure connaissance des marchés, lois, techniques, etc., nécessaires à la réalisation de délits économiques. Il sert également à l'identification des opportunités criminelles.

Le crime économique est influencé par les nouvelles technologies qui deviennent un facteur de production des organisations criminelles et place l'information au cœur de leurs stratégies et processus de décision.

Les nouvelles technologies facilitent toute sorte de vol, modifications, sabotage d'information ou de fraudes. Les phénomènes de chantage, d'extorsion, de racket, de demandes de rançons existent dorénavant sur l'internet.

En effet, les ressources informatiques deviennent les otages potentiels des cybercriminels. Les maîtres-chanteurs se sont approprié le cyberespace et tout le monde peut être la cible de tentatives de chantage, de désinformation ou de cyberpropagande. Par ailleurs, l'explosion du phénomène d'usurpation d'identité depuis 2003, démontre que les criminels ont bien compris l'avantage qu'ils pouvaient tirer, non seulement des capacités d'anonymisation offertes par l'internet mais aussi, de l'appropriation des fausses identités afin de ne pas être poursuivis ou tenus responsables d'actions criminelles ou terroristes. L'usurpation d'identité, aisément réalisable sur l'internet, favorise la réalisation d'activités illicites.

Comme tous les criminels qui profitent des infrastructures technologiques mises en place, les blanchisseurs de fonds recourent de plus en plus à l'internet afin de pouvoir utiliser légalement des capitaux générés par les activités criminelles telles que le trafic de drogue, la vente illégale d'armes, la corruption, le proxénétisme, la pédophilie, la fraude fiscale, etc.

Bien qu'il soit largement sous-déclaré, et le plus souvent méconnu, le blanchiment d'argent via l'internet prend de l'ampleur. L'internet offre un potentiel exceptionnel tant par la dématérialisation (anonymat, monde virtuel, rapidité de transfert) que par la non-territorialité (phénomène transnational, conflits de compétences et de juridictions), caractéristiques largement exploitées par les acteurs traditionnels du blanchiment. L'internet permet en toute impunité, la réinsertion de l'argent sale dans les circuits économiques par le biais de transferts de flux, d'investissement et de capitalisation.

Les placements boursiers en ligne, les casinos en ligne, le e-commerce – ventes de produits et services fictifs contre paiement réel, générant des bénéfices justifiés, de telles activités sont incontrôlables et les poursuites en justice impossibles, le e-banking, les transactions du foncier et de l'immobilier *via* le net, la création de sociétés virtuelles «écran», les porte-monnaie électroniques sont utilisés pour effectuer le crime des crimes qu'est le blanchiment. En ayant recours à certains services dématérialisés, l'internaute, peut favoriser inconsciemment le développement du blanchiment d'argent. Les entreprises peuvent également être fortuitement impliquées dans ce processus, et en subir des conséquences judiciaires et commerciales qui peuvent être importantes. Cela constitue alors un risque majeur pour les entreprises.

Actuellement, il existe peu de moyens efficaces pour maîtriser ce phénomène du blanchiment via les nouvelles technologies.

II.1.5 Banalisation de la cybercriminalité et extension de la criminalité

La cybercriminalité se réalise le plus souvent au travers de délits ordinaires, presque invisibles mais très présents et efficaces, du fait de la mise en réseau des ressources et des personnes. Les entreprises mais surtout leurs ressources informatiques et informationnelles deviennent des cibles privilégiées pour les organisations criminelles à la recherche de profits. Il s'agit alors d'une menace stratégique dans la mesure où l'argent se trouve dans les systèmes informatiques, dans les grandes entreprises, dans des fonds de pension, etc., et non seulement dans les banques.

L'ouverture de l'internet via des serveurs web, des portails, où la messagerie électronique expose l'entreprise au risque d'origine criminel et permet le positionnement d'acteurs criminels à son contact. L'internet est un outil de communication mais il est aussi un environnement chaotique, complexe, dynamique et hostile qui peut constituer un outil de déstabilisation et de réalisation de délits. L'internet peut être alors considéré comme étant une zone criminalisée. Or, du fait de la nécessité pour les institutions d'être présentes sur l'internet, nous sommes en droit de nous demander si ces dernières ne contribuent pas dans une certaine mesure à l'extension de la criminalité sur l'internet.

La sécurité intérieure d'un pays est aujourd'hui confrontée à des formes d'expression de menaces criminelles liées à l'existence des technologies de l'information. Les technologies de l'internet sont au cœur de la guerre de l'information (infoguerre *infowar*) dont les enjeux sont avant tout d'ordre économique et les impacts importants pour le bon déroulement des activités. L'internet permet non seulement la manipulation de l'information mais est aussi un outil privilégié pour répondre des rumeurs ou toute forme d'intoxication ou de campagne de déstabilisation. De même, sont facilitées les activités d'espionnage et de renseignement, puisqu'il est devenu aisé d'intercepter des informations transférées sur l'internet.

II.1.6 Cybercriminalité et terrorisme

La cybercriminalité peut avoir une dimension terroriste dans la mesure ou les systèmes attaqués sont impliqués dans des infrastructures critiques. En effet, les infrastructures essentielles au bon fonctionnement des activités d'un pays (énergie, eau, transports, logistique alimentaire, télécommunications, banque et finance, services médicaux, fonctions gouvernementales, etc.), voient leur vulnérabilité augmentée par un recours accru aux technologies de l'internet.

Il faut souligner l'importance des systèmes de production et de distribution d'électricité car ils conditionnent le fonctionnement de la plupart des infrastructures. La prise de contrôle d'infrastructures critiques semble être un des objectifs du cyberterrorisme, la preuve en est la recrudescence de *scans* (tests de systèmes informatiques pour découvrir leurs vulnérabilités afin de pouvoir les pénétrer ultérieurement) dirigés sur des ordinateurs d'organisations gérant ces infrastructures.

A ce jour, la définition du cyberterrorisme n'est pas claire. Le plus simple serait sans doute de considérer le cyberterrorisme comme du terrorisme appliqué au cyberespace. Or, dans son sens courant, le terrorisme fait référence à l'emploi systématique de la violence pour atteindre un but politique.

Nous sommes en droit de nous demander si l'arrêt éventuel de l'internet ou d'une partie de l'internet, suite à des actes de malveillance, serait susceptible de provoquer la terreur au sein de la communauté des internautes, de certains acteurs économiques particuliers, de la population.

Ne s'agirait-il pas, le plus souvent, de terrorisme économique visant à porter préjudice aux organisations qui réalisent des activités au travers de l'internet?

Il faut être prudent quant à l'usage du terme «cyberterrorisme» qui s'est répandu depuis le 11 septembre 2001. En effet, souvenons-nous que les premiers dénis de services distribués (DDOS) largement médiatisés furent le fait d'un adolescent de 15 ans (Mafia Boy) le 10 février 2000. Identifié et appréhendé plusieurs mois plus tard, bien qu'il n'ait pas rendu publique sa motivation, tout laisse à penser qu'elle n'était pas politique.

Est-ce que cette même attaque perpétrée après le 11 septembre 2001, n'aurait pas été aussi qualifiée de cyberterrorisme?

En l'absence d'éléments concrets, sans revendication ni auteur présumé d'une attaque, il est difficile de qualifier une attaque de cyberterroriste.

Le terme de cyberterrorisme recouvre une réalité assez floue dans le répertoire des nouvelles menaces et il est difficile à priori de supposer la motivation et les objectifs d'un agresseur ou d'un groupe d'agresseurs inconnus. En effet il est parfois malaisé de distinguer en fonction de la cible uniquement, les motivations d'un délinquant, d'un terroriste, d'un mercenaire, d'un militant, d'un escroc ou encore d'un immature.

Le type d'agression informatique ne suffit pas à définir avec certitude la motivation ou les objectifs d'un malveillant. Ceci constitue une des difficultés de la lutte contre le crime informatique car il est nécessaire de disposer d'informations complémentaires pour caractériser l'intention criminelle.

Que cela soit au travers des processus de déstabilisation économique, par la mise en péril d'infrastructures critiques, par la propagation d'idéologies ou par de la manipulation d'information, le cyberterrorisme constitue une nouvelle forme de menace qui est à considérer de manière très sérieuse. Au-delà des systèmes informatiques et du monde virtuel que symbolise l'internet, la vie peut être menacée en portant indirectement préjudice à l'intégrité des personnes.

II.1.7 Cyberdélinquants

Parvenir à distinguer la motivation du cyberdélinquant, ainsi que son niveau de technicité, permet, d'évaluer la gravité d'une attaque et ainsi de mieux la contrer. Sécuriser un système d'information nécessite de connaître contre qui l'on doit se protéger. De nos jours, on observe deux grands types de cyberdélinquants à savoir, d'une part, les professionnels dont les activités sont directement rémunératrices et, d'autre part, les amateurs, généralement animés par un fort besoin de reconnaissance sociale (Figure II.4).

Les professionnels sont généralement:

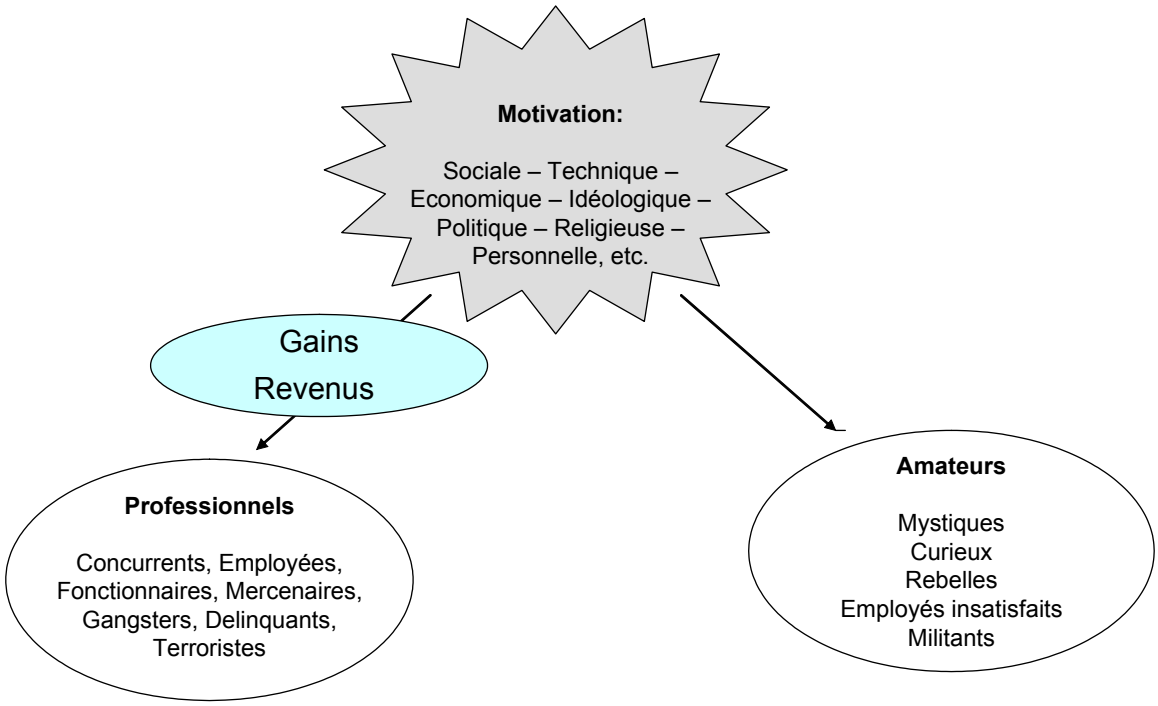
- des concurrents directs de l'organisation visée;
- des fonctionnaires au service de leur Etat;
- des mercenaires (pouvant agir aussi bien pour le compte d'institutions privées que publiques);
- des truands de toutes sortes.

Parmi les amateurs, se reconnaissent:

- les techniciens, successeurs des premiers passionnés, ces hackers des premiers âges dont la motivation essentielle était le désir de maîtriser toujours mieux les technologies;
- les curieux;
- les immatures: souvent appelés «script-kiddies» ou «kiddiots». Ils sont fréquemment sur le devant de la scène après avoir été attrapés. Le fait qu'ils soient pris par les forces de l'ordre ne signifie pas nécessairement qu'ils sont les seuls cyberdélinquants;

– les psychopathes;
– les militants, mus par idéologie ou religion, qui sont d'ailleurs souvent à cheval entre amateurisme et professionnalisme).

Figure II.4 – Deux grandes familles de cyberdélinquants



Les motivations fondamentales de ces personnes sont relatives à des composantes d'ordre social, technique, politique, financière ou étatique.

La motivation sociale trouve ses racines dans le besoin de reconnaissance par ses pairs de l'individu, lié généralement à une structure de bande. Il veut prouver sa valeur au groupe en se référant aux critères culturels internes. Il s'agit, d'un phénomène analogue à celui des «*taggers*», et qui est relié à une vision très primaire des rapports sociaux. On le retrouve fréquemment chez les immatures pour lesquels le «*hacking*» apporte un sentiment de supériorité et de contrôle d'institutions qu'ils estiment subir dans leur quotidien.

La motivation technique reste rare. Elle a pour objet premier la recherche des limites de la technologie, afin d'en mettre en lumière les limites et les faiblesses et d'en mieux comprendre les atouts.

La motivation politique consiste à créer un événement propre à alerter les médias, pour les focaliser sur un problème grave en espérant provoquer une prise de conscience collective qui amènera sa résolution. Il est à noter alors que la frontière avec le terrorisme peut être ténue, au moins d'un point de vue conceptuel. On doit également souligner que bon nombre de personnes dissimulent leur motivation sociale derrière un objectif politique.

La motivation financière peut s'avérer très forte et sous-tend beaucoup d'actions illicites. L'appât du gain, permet à des criminels en col blanc de s'exprimer via le réseau internet (voleurs, escrocs, concurrents déloyaux, etc.).

Enfin, on peut distinguer une motivation gouvernementale. Qu'il s'agisse de guerre de l'information ou d'espionnage, elle concerne des services administratifs agissant pour le compte de puissances étatiques.

Les délinquants ont su s'adapter aux nouvelles technologies pour faire fructifier leurs activités traditionnelles. On peut légitimement s'inquiéter en voyant à quel point ils peuvent être créatifs lorsqu'il s'agit d'inventer de nouveaux usages pour ces technologies.

II.1.8 Programmes indésirables ou malveillants

II.1.8.1 Spam

Le *spam* est un envoi massif de messages électroniques non sollicités dont la finalité est à l'origine commerciale et publicitaire afin d'inciter les internautes à commander un produit ou un service.

Le *spam* en dépit du déploiement de moyens techniques et des sommes investies par les fournisseurs de service pour le bloquer, malgré également l'annonce faite par les autorités de vouloir combattre ce fléau et les condamnations de spammeurs prolifiques, le *spam* continue à être une véritable nuisance. En septembre 2003 le spam représentait 54% du trafic total des messages électroniques échangés. En 2005 aux Etats-Unis, selon IDC, le nombre de *spams* envoyés a dépassé les 12 milliards de messages, soit 38.7% du trafic total.

Poussé à l'extrême, le phénomène de *spam* peut ressembler à une attaque par bombardement, inondation de messages (*email bombing*) entraînant une surcharge inconsidérée des serveurs de messagerie, des boîtes à lettres des utilisateurs et des désagréments. Cela peut se réaliser par l'inscription de l'utilisateur à son insu à des listes de diffusion d'information (*list linkink*). Ce dernier doit alors se désabonner de ces listes ou, si cela lui semble trop fastidieux, changer d'adresse électronique. Cette alternative, quoiqu'efficace est également dérangeante dans la mesure où il est nécessaire de prévenir tous les interlocuteurs de cette modification d'adresse.

Le nombre de messages non sollicités, inappropriés, ou parfois à contenu propre à choquer en quantité massive peut porter atteinte au respect de la sphère privée de l'internaute (notion de *junk email*). Mais il est constaté que, de plus en plus, le *spam* est utilisé pour propager des programmes malveillants, ce qui lui confère un degré de nuisance sans précdent.

II.1.8.2 Programmes malveillants

Les principaux observateurs de la sécurité informatique que cela soit le CERT[12], le FBI, ou encore le Clusif, constatent dans leurs rapports annuels concernant la criminalité informatique, une augmentation des programmes malveillants ou indésirables s'exécutent à l'insu de l'utilisateur.

Il s'agit des logiciels suivants:

- Les téléchargeurs et implanteurs (downloaders) qui permettent le téléchargement de données (accès à distance et chargement de programmes ou récupération de données);
- Les keyloggers qui sont des enregistreurs de frappe, renifleurs de clavier qui capturent les informations saisies au clavier par l'utilisateur. Il existe également des périphériques matériels, (keyloggers matériels) indétectables par les logiciels qui enregistrent les données;
- Les bot-robots qui sont des programmes permettant la prise de contrôle à distance de systèmes afin de former un réseau d'attaques caché. De 25-50 nouveaux robots sont découverts chaque jour. Ils servent de relais de spamming, de phishing ou pour distribuer des adwares. En octobre 2005, la police hollandaise à arrêtée trois hommes soupçonnés de diriger un réseau de 100 000 ordinateurs – robots qui se proposaient de mener des attaques de déni de service et s'intéressaient aux comptes PayPal et Ebay de leurs victimes;[13]
- Les logiciels publicitaires (adware – advertising software) qui permettent entre autres la personnalisation des démarches commerciales;

---

12 CERT: *Computer Emergency Response Team*; www.cert.org – Statistiques 1998 – 2005 www.cert.org/stats/cert_stats.html

13 Source: Clusif Panorama de la cybercriminalité rapport 2005: www.clusif.asso.fr/fr/production/ouvrages/pdf/PanoCrim2k5-fr.pdf

– Les logiciels espions (spyware – spying software) qui, comme leur nom l'indique, enregistrent des données à l'insu de l'utilisateur. Selon l'éditeur de logiciels Webroot INC. plus de 100 000 différents spywares sont présents sur le net et plus de 300 000 sites internet hébergent de tels logiciels. Un PC connecté sur l'internet possède en moyenne 28 spywares installés à l'insu de son utilisateur. Plus de 80% des ordinateurs d'une entreprise contiennent au moins un spyware. Ces programmes sont à l'origine de 70% des attaques.

A ces logiciels, il faut ajouter les virus et ses dérivés (vers, cheval de Troie, bombe logique).

Les virus sont des programmes malveillants introduits dans un système à l'insu des utilisateurs, qui possèdent la capacité de se dupliquer soit à l'identique, soit en se modifiant (virus polymorphe), de porter atteinte aux environnements dans lequel ils s'exécutent et de contaminer les autres avec lesquels ils sont en relation. Différents types de virus sont distingués en fonction de leur signature, de leur comportement, de leur type de reproduction, d'infection, de dysfonctionnements induits, etc.

L'objet d'un virus informatique, de manière analogue au virus biologique, est de se reproduire et de se propager d'un ordinateur à un autre, en s'attachant à toutes sortes de programmes, le plus souvent à des messages électroniques. Généralement via une intervention humaine. L'exécution d'un virus peut porter atteinte à l'intégrité des ressources informatiques contaminées. Certains peuvent être juste dérangeants, d'autres carrément destructeurs, conduire à des pertes de disponibilité et de confidentialité.

Le terme de virus désigne de manière générique tout programme informatique capable de nuisance (infection, destruction, détournement de ressources, etc.), capable de se reproduire et de se propager.

Environ 50 000 nouveaux virus ont circulé, en 2005[14]. Le virus HTML_NETSKY.P par exemple, répertorié par le *World Virus Tracking Center*, a infecté près de 855 244 machines dans le monde depuis avril 2004. Le coût pour les entreprises infectées par des virus, pour l'année 2004 selon *Computer Security Institute* est de l'ordre de 42 millions USD. Selon F-secure.com il y aurait 4000 virus par jour en circulation.

Les vers, chevaux de Troie, bombes logiques sont des codes malveillants de la famille générique des virus.

Les vers sont des programmes qui se diffusent à travers le réseau, le plus souvent indépendamment d'une intervention humaine et ont souvent comme finalité de consommer de manière excessive des ressources (mémoire, bande passante) portant atteinte ainsi au critère de disponibilité ou favorisant la prise de contrôle à distance des systèmes infectés.

Les programmes malveillants qualifiés de chevaux de Troie (*Troyan horse*) sont introduits subrepticement, souvent sous couvert de programmes anodins ou d'aide, dans des systèmes pour en prendre le contrôle afin de réaliser le vol de temps processeur, l'altération, la modification, la destruction des données et programmes, des dysfonctionnements, des écoutes illicites, mais aussi pour réaliser d'autres malveillances et servir de relais à des attaques ultérieures.

Les bombes logicielles (*logical bomb*) sont des virus qui s'activent lors de la réalisation d'évènements particuliers (date anniversaire par exemple) pour porter atteinte au système dans lequel il se trouve.

En revanche, un bogue (*bug*) dont le terme est d'origine anglaise illustre une erreur de programmation. Par extension défaut de conception ou de réalisation se manifestant par des anomalies de fonctionnement.

En principe, les virus se propagent et s'exécutent si l'utilisateur les active en exécutant les programmes dans lesquels ils résident. La majorité des virus se sont jusqu'à présent propagé via les fichiers attachés aux messages électroniques (*email attachement*) et activé lorsque l'utilisateur double clique dessus et les ouvre.

---

14 Source: IPA/ISEC Computer virus incident report.

Un grand nombre de programmes malveillants existent sous couvert d'outils d'aide à la navigation, à la connexion, à la personnalisation des services, etc., mais en réalité ils sont pour la plupart des outils de capture d'informations (vol d'informations, capture de mots de passe, de trafic), d'appropriation de ressources ou d'attaques. Ils permettent de diffuser et de piloter des outils d'attaques en déni de service distribué (DDoS). Plusieurs milliers sont actuellement en circulation avec comme finalité le profit financier.

Les attaques qualifiées de déni de service (DOS *Denial of Service*) ou de déni de service distribué (DDoS *Distributed Denial of Service*) sont celles qui portent atteinte à la disponibilité des ressources. Elles sont généralement réalisées en sollicitant de manière excessive les services normalement offerts par un serveur, mettant le système dans l'impossibilité de rendre le service pour lequel il est conçu (d'où le nom de déni de service). Du fait du caractère «normal» de la demande de service, une attaque par déni de service est très difficile à contrer (ce qui met à mal l'infrastructure est le nombre considérable de requêtes sollicitées). Elle est d'autant plus difficile à contrer qu'elle est réalisée à partir de plusieurs points ou de systèmes (notion d'attaque par déni de service distribué).

Les vecteurs d'introduction de logiciels malveillants peuvent être des logiciels gratuits ou en démonstration, les sites pornographiques ou de jeux, mais aussi le courrier électronique, le spam et les forums de discussions.

Quel que soit leur mode d'introduction, même s'ils sont installés après un consentement initial ou accord implicite de l'utilisateur, ce qui peut être le cas des *adware* mais jamais des *spyware*, leur usage est détourné. Le plus souvent, ils s'exécutent en l'absence de consentement des utilisateurs. Ces logiciels collectent et transfèrent des données à l'insu de l'utilisateur (observation des habitudes de navigation pour des publicités ciblées) et peuvent servir d'intermédiaires à des activités illégales (relais de *spam* et de *phishing* par exemple) à des fins d'enrichissement de l'entité qui en est à l'origine. La détection désinstallation de tels logiciels est parfois difficile. De manière générale, l'internaute ne possède pas les compétences ou les outils nécessaires pour maîtriser ce risque.

Le phishing consiste à utiliser la messagerie électronique pour leurrer et inciter les internautes à livrer des informations sensibles exploitées ensuite à des fins malveillantes (escroquerie et/ou détournement d'information). En septembre 2005 plus de 5259 sites de *phishing* étaient actifs, ciblant près de 110 marques selon le Journal du net 26.01.2005[15].

Le terme *phishing* est employé pour désigner une technique qui consiste à leurrer les internautes (souvent par le biais d'un message électronique) afin de les inciter à livrer des informations sensibles ou personnelles, (généralement en leur demandant de se connecter sur un site web qui ressemble au site web de l'institution qu'ils connaissent et à remplir des formulaires qui sont alors à disposition des malveillants).

Les informations communiquées par l'internaute, notamment son identité virtuelle, seront ensuite utilisées pour réaliser des malveillances escroquerie, fraudes, etc., au nom des internautes leurrés.

Par analogie à la pèche à la ligne (*fishing*) qui se réalise via un hameçon et un leurre, la pèche électronique aux données sensibles passe par un appât qui amène l'utilisateur à donner de son plein gré l'information convoitée par les malveillants.

Bien que la plupart du temps les tentatives de *phishing* se réalisent par la réception d'un message qui semble authentique et qui est censé être émis par une institution réelle avec laquelle l'internaute est en contact (poste, banque, commerçant, site de ventes aux enchères par exemple), il peut être réalisé par téléphone ou directement par une personne ou encore via le téléphone portable ou une application de messagerie instantanée (*Instant Messaging,* IM).

---

15 www.journaldu net.com

II.1.8.3 Tendances

De nos jours, les virus n'ont plus pour objectif principal la destruction massive et gratuite de données. Ils deviennent pragmatiques et sont orientés vers la recherche de gains. Leur finalité est bien plus intelligente qu'à leur origine et leur capital embarqué leur permet de réaliser des fraudes. Les virus deviennent des vecteurs de réalisation de la criminalité financière au service le plus souvent, de la criminalité organisée et constituent des moyens d'enrichissement considérable pour leur auteur.

Pour ce qui concerne par exemple l'augmentation du spam et des nuisances associées, le CLUSIF[16] a relevé qu'AOL aurait filtré 500 milliards de messages de spam en 2003 et que le spammer le plus prolifique du monde, révélé en décembre 2003 par l'association anti-spam Spamhaus[17], aurait envoyé 70 millions de messages électroniques en un seul jour!

Toujours selon le CLUSIF, aux Etats-Unis, en mai 2003 le «*Buffalo spammer*» a été condamné à payer une amende de 16,4 millions USD au fournisseur de service internet Earthlink, pour avoir envoyé 825 millions de messages non sollicités. Selon Ferris Research le spam aurait coûté au monde des affaires en 2003, 2.5 milliards USD aux Européens et 8.9 milliards USD aux Américains. Ajouté aux 500 millions USD investis par les fournisseurs de service pour bloquer le spam, cet usage abusif de la messagerie électronique devient un véritable problème que l'on ne peut plus ignorer.

Outre les pertes directes consécutives à une fraude, il faut considérer les coûts engendrés par une interruption de service, entraînant une non continuité des opérations, une perte de volume de ventes, les dommages collatéraux, la perte d'image, de réputation, etc., ainsi que les coûts relatifs à la restauration des systèmes dans leur état opérationnel. Ceci représente des sommes non négligeables pour les organisations ciblées par des attaques informatiques.

Ainsi, il est remarqué que le nombre d'attaques ne cesse de croitre, que les virus informatiques constituent de véritables pandémies. Les phénomènes d'usurpation d'identité prennent de l'ampleur et deviennent de plus en plus sophistiqués, comme d'ailleurs les fraudes, escroquerie et diverses formes de chantage qui sont des réalités quotidiennes du cyberespace. Cela affecte tout le monde et touche tous les secteurs d'activité indépendamment des barrières géographiques ou temporelles.

Touts, les systèmes, toutes les plateformes matérielles et logicielles, tous les systèmes d'exploitation, sont touchés sans exclure les systèmes permettant la mobilité des utilisateurs (ordinateurs et téléphone portables).

II.1.9 Principaux délits favorisés via l'internet

II.1.9.1 Escroquerie, espionnage et activités de renseignement, trafics divers, chantage

Tous les crimes et délits «communs» (*racket*, traitent des êtres humains, escroquerie, vol, etc.) que les organisations criminelles commettent, sont susceptibles de bénéficier de l'utilisation des nouvelles technologies de l'information et notamment de l'internet. De manière générale, le service de mise en relation offert par le réseau internet favorise l'ensemble des trafics possibles que cela soit relatif au trafic d'armes ou à celui d'êtres humains, aux escroqueries (atteintes contre des biens, atteintes à des systèmes et infrastructures informatiques, vol de données, atteintes au droit d'auteur, etc.).

L'internet permet aux escrocs de sévir selon diverses modalités. Il y a tous ceux qui usurpent une identité afin de bénéficier de prestations sans avoir à les rémunérer. Leur outil de travail est souvent le logiciel de «*carding*» qui permet de créer de numéros de carte bancaire parfaitement valides bien que ne correspondant à aucun compte réel. Il suffit ensuite d'acheter en ligne et de se faire livrer à une adresse

---

16 CLUSIF – Club de la Sécurité des Système d'Information Français
www.clusif.asso.fr

17 Association Spamhaus: www.spamhaus.org

de complaisance que l'on utilisera une seule fois. Le coût sera supporté par le système bancaire ou le commerçant. L'utilisateur final est aussi concerné lorsque son numéro de carte de crédit a été livré par un *pickpocket*, ou un commerçant indélicat, à un réseau spécialisé.

Une autre famille d'escrocs est constituée par tous ceux qui proposent des prestations inexistantes (vente de diplômes, de passeports diplomatiques d'Etats imaginaires, vente aux enchères de produits inexistants, etc.).

De même, sont facilitées les activités d'espionnage et de renseignement puisqu'il est devenu aisé d'intercepter illégalement, des informations transférées sur l'internet.

Remarquons que l'utilisation systématique de moyens de communication et de sécurité informationnelle comme le chiffrement, par des terroristes professionnels, peuvent aussi améliorer leur propre sécurité en limitant la quantité d'information susceptible d'être récupérée par la police.

L'internet est un puissant medium qui favorise la diffusion de méthodes permettant la réalisation de crimes et de délits, ce qui facilite pour certains le passage à l'illégalité.

II.1.9.2 Atteintes aux personnes

L'internet permet à des communautés virtuelles clandestines, de se constituer autour de pratiques rigoureusement punies par la loi. Il peut s'agir de pornographie, de pédophilie, ou de *snuff movies* (films montrant des scènes de violence et de torture réalisées sur des victimes, pouvant conduire à la mise à mort des personnes maltraitées). Ce type d'activité est en général lié à la traite d'êtres humains qui le plus souvent sont des femmes ou des enfants. Les échanges de films ou de photos sont beaucoup moins faciles à intercepter par la police. De plus, le fait que des serveurs soient localisés dans des pays où les forces de police sont inexistantes ou dépassées ainsi que l'usage du chiffrement ou de serveurs IRC (*Internet Relay Chat*) privés et actifs pendant des durées très limitées, des échanges P2P (*peer to peer*) accroissent la liberté d'action des criminels.

Ces activités illicites tombent sous le coup du droit commun. On peut alors s'interroger si leur commission quasi industrialisée et à grande échelle, que l'internet ainsi que la mobilité des personnes et biens autorisent, ne les transforment pas en de véritables crimes contre une partie de l'humanité?

Atteintes aux personnes. Pour ce qui concerne les atteintes à la personnalité, retenons par exemple: Atteinte à la vie privée, à la représentation de la personne, au secret professionnel, aux droits de la personne résultant des fichiers ou traitements informatiques. Pour ce qui concerne les atteintes aux mineurs retenons la diffusion de messages pornographiques susceptibles d'être vus par des mineurs.

II.1.9.3 Contrefaçon

La facilité avec laquelle l'information numérique peut être reproduite, a contribué à l'apparition d'un marché de la copie illicite. Cela représente un manque à gagner de plusieurs dizaines de milliards USD, pour les différents éditeurs dans les domaines des logiciels, de la musique ou encore du film vidéo par exemple.

Par ailleurs, on constate une augmentation très importante du nombre de travaux scolaires ou universitaires réalisés par simple copie de documents existants sur le web.

Les infractions au code de la propriété intellectuelle peuvent être nombreuses: contrefaçon d'une œuvre de l'esprit (y compris logiciel), de dessin, d'un modèle, d'une marque, etc.

II.1.9.4 Manipulation de l'information

La manipulation peut prendre diverses formes, comme par exemple la diffusion de documents internes d'une entreprise de manière à provoquer sa déstabilisation, envois de courriers électroniques appelant les destinataires à réaliser des dons monétaires sur des sites contrefaits, etc.

L'internet est un outil privilégié pour répandre des rumeurs ou toute forme d'intoxication. Il favorise également les infractions de presse, la provocation aux crimes et délits, l'apologie de crimes contre l'humanité, apologie et provocation au terrorisme, provocation à la haine raciale, négationnisme, diffamation, injure, etc.

La Figure II.5 donne quelques exemples de délits facilités par l'internet.

Figure II.5 – Exemples de délits facilités par l'internet

Crimes et délits contre les personnes – Atteintes à la personnalité – Atteinte à la vie privée – Atteinte à la représentation de la personne – Dénonciations calomnieuses – Atteinte au secret professionnel – Atteinte aux droits de la personne résultant des fichiers ou des traitements informatiques – Atteintes aux mineurs, etc.
Crimes et délits contre les biens – Escroquerie – Atteintes aux systèmes informatiques – Infraction de Presse
Provocation aux crimes et délits – Apologie des crimes contre l'humanité – Apologie et provocation au terrorisme – Provocation à la haine raciale – Négationisme – Diffamation – Injures
Infraction au code de la propriété intellectuelle – Contrefaçon d'une œuvre de l'esprit (y compris logiciel) Contrefaçon d'un dessin ou d'un modèle – Contrefaçon de marques – Participation à la tenue d'une maison de jeux de hasard (cybercasino)

II.1.9.5 Rôle des institutions publiques

Les institutions publiques ont plus que jamais le besoin de jouer leur rôle traditionnel de poursuite et de répression des fraudes et des délits. Elles devraient aussi être actives en matière de sensibilisation et d'information de la population. Il serait notamment utile de pouvoir disposer d'éléments de référence relatifs à la protection des personnes et des biens lors de l'usage de l'internet.

De plus, il serait dangereux de laisser les forces de police prendre un retard dans le domaine technologique. En effet, un éventuel effort de rattrapage après quelques années aurait non seulement un coût financier direct, sous forme d'investissements dans de nouvelles infrastructures, mais aussi et surtout un coût social par l'accroissement de l'emprise des structures mafieuses ou assimilées sur la société, avec tous les risques de déstabilisation que cela comporte.

Toutefois, l'accroissement excessif de la présence policière sur le réseau n'est pas forcément la meilleure des choses et peut entrer en conflit avec les besoins de confidentialité des échanges et de respect de la sphère privée des individus.

II.1.10 Incidents de sécurité et chiffre noir de la cybercriminalité

Il convient de remarquer que peu de statistiques relatives à la cybercriminalité sont disponibles. Il s'agit d'un nouveau champ d'expression de la criminalité où peu d'affaires sont reportées à la police. De plus, ces infractions se perpétuent au niveau mondial; or les législations pénales sont nationales, il est alors parfois difficile de mettre en commun des statistiques traitant de délits dont la qualification peut varier d'un pays à un autre. Ainsi par exemple lorsqu'un système informatique est utilisé afin de réaliser une transaction financière frauduleuse après usurpation des paramètres de connexion d'un utilisateur: est-ce un crime informatique ou un crime financier?

Néanmoins, la mise en place par exemple, aux Etats Unis de «*Computer Investigation and Infrastructure Threat Assessment* (CITA) *squads*» décentralisés et coordonnés par le *National Infrastructures Protection Center* (NIPC) relève indirectement l'ampleur de la cybercriminalité.

Le nombre d'incidents de sécurité rapportés au CERT[18] continue de progresser depuis le début des années 2000 et le nombre d'attaques déclarées aux autorités judiciaires tend également à augmenter au cours des années, ce qui contribue à une meilleure connaissance et prise en compte de la criminalité informatique. L'année 2003 a été marquée par l'augmentation significative du volume du spam, qui ne se limite plus à l'internet mais touche également les SMS, et par l'arrestation et la condamnation de spammers. Des opérations de police d'envergure que cela soit aux Etats Unis (opération E-Con en mai 2003, Cyber-Sweep en octobre 2003 qu'en Europe (Espagne, Italie, France, GB, etc.) montrent que les autorités réagissent et s'adaptent à ce nouveau contexte criminel. L'arrestation et la condamnation de quelques auteurs de virus ou de spam démontrent la volonté de restreindre ces nouvelles formes de nuisance. Toutefois, le nombre de condamnations reste très marginal au regard de l'importance quantitative du spam et des virus circulants journellement[19].

Le chiffre noir de la cybercriminalité est difficile à appréhender. Seulement 12% des cybercrimes seraient connus des instances de justice et police et du grand public[20]. Il existe une réelle difficulté à obtenir un état des lieux réaliste de la criminalité informatique, ce qui constitue un véritable obstacle à l'analyse du phénomène et contribue à la méconnaissance de son ampleur.

Le manque de statistiques officielles provient en partie du fait que les organisations:

- ne souhaitent pas forcément communiquer sur les malveillances subies;
- ignorent qu'elles sont victimes d'une malveillance, notamment pour toutes attaques passives (détournement transparent de données, de flux, écoutes clandestines, introduction non détectée dans des systèmes, etc.), ou en prennent conscience qu'à posteriori lorsque toute action de réaction devient obsolète;
- ne savent pas gérer une situation de crise;
- n'ont pas une confiance suffisante dans les instances de justice et police et dans leur compétence pour traiter ce type de problème;
- préfèrent faire justice elles mêmes.

L'expertise des attaquants, la sophistication et l'efficacité des attaques, les boîtes à outils, les outils d'attaques ainsi que le nombre d'attaques ne cessent de croître. Ce dynamisme induit une complexité croissante du phénomène à maîtriser. Sans une volonté politique forte et une responsabilité de tous les acteurs au niveau international et un partenariat efficace des secteurs privés et publics, toute mesure de sécurité, qu'elle soit d'ordre technologique ou législative, ne constituera qu'une approche insuffisante et parcellaire de la sécurité qui sera donc inefficace à la maîtrise de la criminalité informatique.

---

18 CERT Coordination Center, Carnegie Mellon University (http://www.cert.org)

19 85 059 virus connus ont été recensés en décembre 2003 par l'Information Technology Promotion Agency Information Security Center (IPA/ISEC – Japon) – «Computer Virus Incident Reports». 2004. www.ipa.go.jp/security/english/virus/press/200401/virus200401-e.html

20 Vladimir Gobulev «Computer crime typology» – January 09, 2004 – Computer Crime Research Center www.crime- research.org/articles/Golubev1203/

II.1.11 Se préparer à la menace d'origine cybercriminelle: un devoir de protection

Il faut se préparer à la menace d'origine cybercriminelle qui un jour ou l'autre se concrétisera.

Il s'agit d'organiser la protection et la défense des valeurs en prenant en considération la menace du risque criminel lors de la définition de la stratégie de sécurité. Il est parfois difficile d'identifier les acteurs de la cybercriminalité, leurs modalités d'action et leur motivation, mais il est constaté que les organisations criminelles agissent généralement de manière opportuniste et s'attaquent plus volontiers aux acteurs vulnérables. Ne pas devenir une cible prioritaire de la cybercriminalité pour une organisation, est possible dans la mesure ou l'organisation protégera efficacement, c'est-à-dire mieux que les autres, son infrastructure informatique et sortira de la logique ou la mise en place de la sécurité se limite à avoir le même niveau d'insécurité que ses concurrents. Le risque cybercriminel est alors transformé en levier pour réaliser une sécurité de qualité.

En revanche si l'organisation est considérée, par les acteurs classiques de la criminalité, comme étant une source de richesse ou un symbole à détruire, elle sera l'objet d'attaques ciblées. La destruction par des actes terroristes est alors envisageable pour ce qui concerne le deuxième cas. Une stratégie de protection et de défense appropriées doit alors être mise en place. Toutefois, les outils classiques de l'assurance et de la gestion de risques sont de peu d'efficacité pour le risque d'origine criminel, car certains ne peuvent pas être évités à moins de ne pas être connecté à l'internet.

Le risque criminel possède une dimension globale et touche dans leur intégralité (actionnaires, dirigeants, personnel, outil de production, etc.) les institutions. Celles-ci doivent savoir préserver leur intégrité face au risque criminel, comme elles savent se protéger des risques de corruption par exemple. Elles doivent être rentables et compenser le manque à gagner engendré par le risque cybercriminel et le coût des mesures à mettre en place pour le maîtriser. Un modèle économique doit alors être pensé pour supporter de manière optimale le coût de la protection des infrastructures, de la sécurité des systèmes, réseaux, données et services, réalisées au détriment du développement économique, par ceux qui partagent la valeur que les organisations créent.

La prise de conscience de la fragilité du monde numérique et de la non-maîtrise totale non seulement des technologies et infrastructures informatiques et télécoms mais aussi des solutions de sécurité commercialisées, doit nous faire poser la question fondamentale de la dépendance vis-à-vis de technologies que nous ne maîtrisons pas.

Jusqu'où désirons-nous être dépendants d'un fournisseur, d'un pays, d'un administrateur?

Le premier élément de la maîtrise du risque cybercriminel passe avant tout par:

- repenser la relation aux nouvelles technologies et aux fournisseurs;
- l'exigence d'une garantie de sécurité;
- la responsabilité de l'ensemble des acteurs.

Avant de mettre en place des mesures classiques de sécurité par une démarche de prévention – protection – défense, protégeons les ressources sensibles ou critiques d'une organisation en repensant tout d'abord leur relation aux nouvelles technologies.

Exigeons:

- des produits de qualité dont le niveau de sécurité puisse être contrôlable et vérifiable;
- que la sécurité ne soit plus réalisée dans l'obscurité, qu'elle soit transparente;
- que la sécurité ne relève plus uniquement de la responsabilité des utilisateurs mais aussi des intermédiaires techniques – responsabilité juridique des professionnels (concepteurs de programmes, fournisseurs d'accès, etc.);
- qu'un minimum de sécurité soit intégré en mode natif dans les solutions technologiques (notion de produits surs).

Au-delà des préoccupations des organisations, face à la synergie et à la convergence du crime organisé, du crime économique et du cybercrime, une réponse complète, multilatérale et transnationale est à apporter pour renforcer la confiance des acteurs économiques envers les technologies de l'information et diminuer les opportunités criminelles.

Cette réponse doit satisfaire aux besoins de sécurité nationale, des organisations et des individus. Elle doit contribuer à limiter à un niveau acceptable la cybercriminalité, à établir la confiance dans le monde numérique, à minimiser le risque de corruption et de menace des pouvoirs publics.

Chapitre II.2 – Cyberattaques

II.2.1 Caractéristiques des cyberattaques

Plusieurs manières de détourner les possibilités offertes par les technologies de l'internet existent. Elles sont le plus souvent fondées sur l'usurpation de paramètres de connexion, de mots de passe d'ayant droits, ainsi que sur le leurre et l'exploitation de failles et de vulnérabilités des technologies.

II.2.2 Appropriation de mots de passe des utilisateurs pour pénétrer des systèmes

Les principaux moyens qui permettent d'obtenir des paramètres de connexion d'ayants droits pour s'introduire dans des systèmes sont les suivants:

- Obtention directe: le mot de passe est évident (prénom de la personne, du conjoint, de ses enfants, dates de naissance, etc.), le mot de passe est donné directement par l'utilisateur au malveillant.
- Obtention par leurre de l'utilisateur (notion de social engineering): le fraudeur se fait passer pour un administrateur et demander pour des raisons techniques, les mots de passe des utilisateurs qui dans la majorité des cas, les donnent.
- Obtention par écoute du trafic: le fraudeur intercepte, écoute les données transmises en clair par les protocoles de communication (écoute passive (sniffing) surveillance du trafic réseau (monitoring)).
- Obtention par un logiciel: un «cheval de Troie» est introduit dans le poste de travail d'un usager et enregistre à son insu ses paramètres de connexion à des systèmes distants.
- Obtention par accès au fichier de sauvegarde des mots de passe.
- Obtention par déchiffrage (cracker) des mots de passe chiffrés.
- Obtention par observation des utilisateurs par activation des périphériques multimédia pour enregistrer leurs paramètres de connexion.

Une fois en possession des clés d'entrée dans les systèmes (identification du couple l'utilisateur, mot de passe), il est aisé de les pénétrer et d'effectuer toutes sortes d'opérations de lecture ou d'écriture. L'enjeu pour le *hacker* est alors de ne pas se faire détecter et de ne pas laisser la trace de sa présence dans les systèmes visités.

II.2.3 Attaque par déni de service

Une attaque conduisant à un déni ou refus de service peut être réalisée en sollicitant excessivement des ressources. Ne possédant pas la capacité de traiter un tel afflux de demandes, les systèmes ciblés, surchargés par un trop grand nombre de requêtes, s'effondrent et deviennent indisponibles. Elles peuvent être perpétrées en tirant parti des failles de leur système d'exploitation et utiliser par exemple ses caractéristiques internes, notamment celles de leur gestion de certaines zones tampon (*buffer overflow attack*) entraînant des dysfonctionnements graves pouvant conduire à l'arrêt des systèmes.

Une attaque par inondation de messages (*e-mail bombing*) qui consiste à submerger la boîte à lettres électronique d'un utilisateur peut entraîner un déni de service.

II.2.4 Attaque par modification de page web

Une attaque par modification de la page d'accueil d'un site web (*defacement attack*) est réalisée en substituant une page d'un site par une nouvelle, dont le contenu (pornographique, politique, etc.) est variable selon la motivation des attaquants. Une variante de ce type d'attaque, consiste à rediriger l'utilisateur vers un faux site, ressemblant exactement à celui auquel il s'est initialement connecté, afin de lui soustraire par exemple son numéro de carte bancaire. Ce type d'attaque est mis en œuvre lors d'opérations de *phishing*.

Les contenus de sites d'information peuvent également être modifiés à des fins de désinformation (pour influencer le cours d'actions, déstabiliser, manipuler l'opinion publique, etc.). Ces attaques sémantiques (*semantic attack*) qui touchent au sens même des informations, relèvent de l'infoguerre (*infowar*).

II.2.5 Attaques basées sur le leurre et le détournement du mode opératoire des protocoles

Tous les protocoles de la famille TCP/IP (*Transmission Control Protocol/Internet Protocol*) peuvent être détournés et mis en œuvre pour porter atteinte à la sécurité de systèmes. Il en est de même des protocoles et mécanismes qui contribuent à l'acheminement des données au travers du réseau. Ainsi, par exemple, lors de session de travail entre un client et un serveur, un vol de session TCP peut exister.

En effet, le protocole TCP (*Transmission Control Protocol*) pour s'exécuter, établit une connexion logique entre les deux correspondants et supporte l'échange de données applicatif entre ces derniers. Or, pour mettre en relation les applications distribuées, TCP utilise des «numéros de port» (*port number*) ou identifiants logiques des applications. Certains sont spécifiques et réservés à des programmes particuliers et bien connus des utilisateurs; d'autres sont affectés dynamiquement lors de la connexion selon un algorithme déterminé. Une attaque par numéro de port TCP consiste à deviner ou à prédire les prochains numéros de ports affectés à l'échange de données pour les utiliser à la place de l'utilisateur normal et se substituer à lui. Ainsi, on peut «passer» des *firewalls* et établir une connexion «sécurisée» entre deux entités (l'entité pirate et l'entité cible). Bien sûr, l'entité originelle qui a été substituée ne peut pas communiquer avec l'entité distante; il suffit alors, de lui transmettre un message lui signifiant par exemple que le système sollicité est inactif.

Le *User Datagram Protocol* (UDP) est un protocole de niveau 4 (Transport) s'exécutant en mode non connecté. Il constitue une alternative à l'usage du protocole TCP pour le transfert rapide d'un petit volume de données. Les communications UDP ne font l'objet d'aucun contrôle. Le protocole UDP n'effectue pas de contrôle d'identification, de contrôle de flux et de contrôle d'erreur, de ce fait n'importe qui peut utiliser une adresse IP d'un interlocuteur autorisé à se connecter à un système et s'en servir pour le pénétrer. Des vols de sessions UDP peuvent également avoir lieu sans que les serveurs d'application ne s'en rendent compte

Par ailleurs, il est aisé, quand on connaît le mode opératoire des différents protocoles, qui est public, de détourner leur usage, de générer de faux paquets pour surcharger le réseau par exemple et l'inonder pour entraîner des dénis de service. Ainsi, on touche au critère de sécurité relatif à la disponibilité du réseau et des services.

Les délinquants informatiques savent très bien tirer parti des protocoles et de leur limites pour:

- paralyser le réseau;
- rediriger des paquets IP vers une fausse destination (la leur par exemple);
- augmenter considérablement la charge des systèmes en leur faisant traiter, en vain, un grand nombre de messages non significatifs;
- empêcher un émetteur d'envoyer des données;
- contrôler le flux d'émission des paquets, ce qui a également des conséquences sur le trafic supporté par le réseau et porte atteinte à ses performances (fiabilité, sûreté de fonctionnement).

De manière générale, les attaques au niveau du routage se basent sur la mystification des routeurs, des passerelles et des destinataires, en leur fournissant de fausses informations d'adressage qui permettent de détourner les données.

En utilisant par exemple certaines facilités optionnelles du protocole IP qui permettent de définir la route, c'est-à-dire de spécifier les adresses des systèmes intermédiaires par lesquels un paquet doit passer, et en falsifiant ces adresses, un fraudeur peut aisément rediriger des paquets vers une destination de son choix.

Outre le fait que les attaquants savent tirer partie du mode opératoire des protocoles de communication, ils savent également exploiter les caractéristiques des systèmes d'exploitation et de leur mode de fonctionnement. Ainsi, des dépassements de capacités de certaines zones tampon des systèmes (*buffer overflow attack*) entraînent des dysfonctionnements graves pouvant conduire à leur arrêt. Les cibles de ce type d'attaque sont, bien entendu, tous les systèmes jouant un rôle important dans la réalisation de services, que cela soit pour l'acheminement des données comme les routeurs, ou la gestion des noms et des adresses comme les serveurs de noms par exemple. La plupart des attaques dont sont l'objet les sites web sont celles qui les rendent indisponibles et qui peuvent être perpétrées par l'exploitation des failles de leur système d'exploitation.

II.2.6 Attaques contre les infrastructures critiques

Les infrastructures critiques essentielles au bon fonctionnement d'une société (énergie, eau, transports, logistique alimentaire, télécommunications, banque et finance, services médicaux, fonctions gouvernementale, etc.), voient leur vulnérabilité augmentée par un recours accru aux technologies de l'internet qui les rendent accessibles depuis le réseau des réseaux.

De plus, il faut souligner l'importance particulière de la vulnérabilité des systèmes de production et de distribution d'électricité. Ils constituent une infrastructure vitale, donc critique, dans la mesure ou elle conditionne le fonctionnement de la plupart des autres infrastructures. La complexité et le caractère réparti des relations entres les différentes infrastructures critiques est à la fois source de force et de vulnérabilité.

Il est fondamental de sécuriser les passerelles vers l'internet des réseaux de gestion de ces infrastructures et de mettre en place au niveau régional ou national, des organismes chargés de la protection des infrastructures critiques. Leur mission première est de coordonner la conception et la mise à jour des plans de protection de chacune des infrastructures. En effet, la cohérence et la compatibilité de ces plans et solutions de sécurité est primordiale en cas de crise touchant simultanément plusieurs d'entre elles.

II.2.7 Mode de déroulement d'une cyberattaque

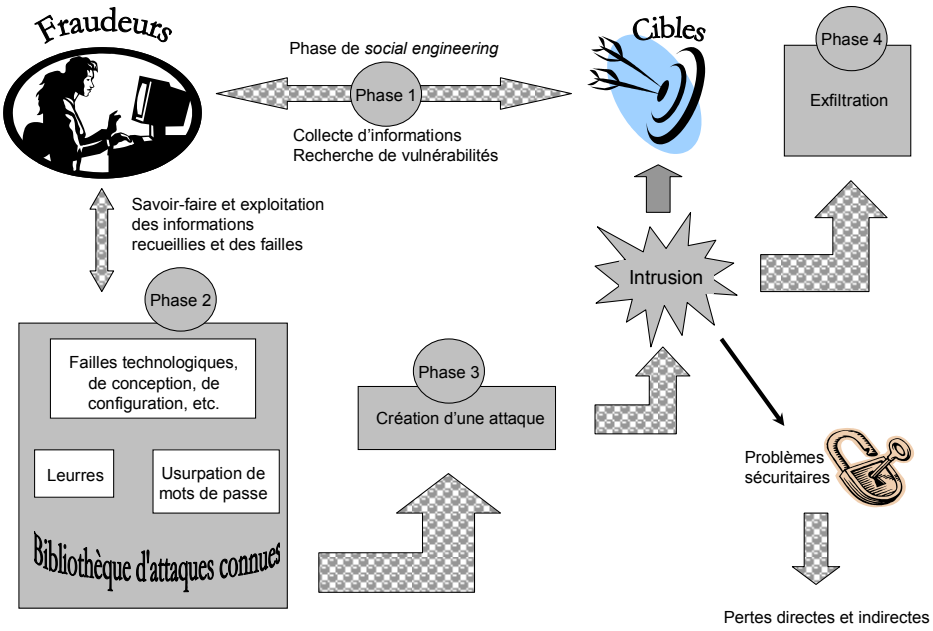
La Figure II.6 présente les différentes phases de déroulement d'une attaque[21].

La première phase de collecte d'informations et de recherche de vulnérabilité d'un système cible a pour objet de récolter le maximum d'informations sur le système ciblé afin de les exploiter. Cela consiste à connaître les mécanismes et niveaux de sécurité en vigueur concernant l'identification, l'authentification, le contrôle d'accès, la cryptographie, la surveillance et à identifier les failles techniques, organisationnelles, humaines de l'environnement. L'attaquant tirera partie le plus souvent de la naïveté ou de la crédulité des utilisateurs pour leur soutirer des informations facilitant la création d'une attaque (notion de *social engineering*).

---

[21] Figure issue du livre «Sécurité informatique et télécoms: cours et exercices corrigés»; S. Ghernaouti-Hélie; Dunod 2006.

Figure II.6 – Phases caractéristiques du déroulement d'une attaque



De plus, le fraudeur s'emploiera à détecter et exploiter les failles de sécurité connues mais non encore réparées (non *patchées*) et à utiliser les outils disponibles (notions de bibliothèques d'attaques ou de boites à outils d'attaques) pour s'introduire dans les systèmes. La phase d'exfiltration a pour objectifs principaux de faire en sorte que l'attaque ne soit pas détectée et que l'attaquant ne laisse pas de trace pouvant servir à son identification. Pour contribuer à cela, il s'emploiera à rester anonyme, à utiliser des alias (pseudonymes), à usurper l'identité numérique d'utilisateurs, ou encore à brouiller les pistes en passant par plusieurs systèmes intermédiaires ou relais.

SECTION III

APPROCHE TECHNOLOGIQUE

Chapitre III.1 – Infrastructures de télécommunication

III.1.1 Caractéristiques

La grande couverture géographique du réseau téléphonique a fait de lui un réseau préférentiel desservant un grand nombre d'utilisateurs. Son infrastructure permet de l'utiliser aujourd'hui, non seulement pour transporter des données vocales, mais également des données informatiques. Ainsi, il est possible, à condition de disposer des interfaces adaptées, de raccorder des ordinateurs via le réseau téléphonique. Par ailleurs des points d'accès au réseau internet se sont développés ces dernières années, les cybercafés continuent à émerger et de plus en plus de pays disposent d'une infrastructure de transport plus accessible et performante. Des réseaux câblés sont parfois déployés pour assurer la transmission de canaux de télévision.

Aux infrastructures fixes de télécommunication, il faut associer celles qualifiées de sans fil qui autorisent la mobilité des utilisateurs, technologies faisant appel aux infrastructures satellitaires et spatiales et à celles recourant aux infrastructures hertziennes terrestres. Ainsi, ces dernières années, la téléphonie mobile offre ses services dans beaucoup de pays en développement.

La norme GSM (Global System for Mobile communication) s'est imposée sur plusieurs continents pour la transmission de la voix et éventuellement de petits volumes de données. C'est la nouvelle génération des réseaux mobiles, spécifiée selon la norme UMTS (Universal Mobile Telecommunication System) qui, en offrant de meilleures performances de transmission, permet un usage plus extensif du téléphone portable multimédia. Toutefois, l'évolution des réseaux GSM, intégrant le service GPRS (General Packet Radio Service), permet d'augmenter les vitesses de transmission afin de mieux satisfaire les besoins des applications informatiques sur des réseaux mobiles.

Par ailleurs, l'irruption des technologies comme le GSM caractérise une mutation tant technologique que comportementale ou économique. En effet, le monde des mobiles constitue un domaine en pleine expansion, s'inscrivant dans un contexte de concurrence mondiale effrénée. Il permet également de pénétrer le marché des télécommunications, jusque là réservé aux opérateurs, par un nouveau service, le radiotéléphone, tout en construisant une infrastructure réutilisable pour tout transfert de données.

Quelle que soit la technologie retenue pour déployer des téléservices, les infrastructures de télécommunication pour les pays en développement doivent permettre:

– un interfonctionnement numérique banalisé (voix, données, image) d'un ensemble défini de services de base facilement réalisables, maintenables et de couverture géographique adaptée (nationale et internationale). Ceci s'inscrivant dans une approche de qualité totale (offre pérenne, stable et granulaire dont le choix peut être réversible à moindre coût technique et économique); et de sécurité optimale;
– une harmonisation technique et commerciale; une protection contre une cartellisation potentielle, pour un développement harmonieux des infrastructures et services, avec une garantie de régulation active des abus des positions dominantes.

III.1.2 Principes fondamentaux

Un réseau de télécommunication est constitué d'un ensemble collaboratif de ressources informatiques et de transmission offrant des services de communication. Ces services permettent de réaliser l'accès distant et le partage des ressources informatiques interconnectées, la mise en relation des applications et des personnes, l'exécution de programmes à distance ainsi que le transfert d'informations.

Disposer d'une infrastructure de communication performante, reliant et autorisant la coopération de toutes sortes d'équipements, d'applications informatiques et de personnes, quels que soient la distance à couvrir, le lieu et la nature des flux d'information à transférer, est devenu impératif pour l'accomplissement des activités économiques.

Les réseaux se distinguent le plus souvent selon plusieurs critères parmi lesquels on peut noter la couverture géographique, la topologie[22], la technologie mise en œuvre et les applications supportées, le mode de fonctionnement, le type de support de transmission (filaire, non filaire), leur nature privée ou publique, etc.

Historiquement, les premiers réseaux furent des réseaux grande distance[23] (réseaux téléphoniques, télex, Transpac, internet, etc.). C'est avec l'arrivée des micro-ordinateurs (début des années 80) que sont apparus les réseaux locaux[24].

Depuis quelques années, ces distinctions tendent à s'atténuer dans la mesure où les réseaux sont reliés entre eux. Un réseau local, par exemple, peut s'interconnecter à d'autres et devenir un réseau étendu. Par ailleurs, les réseaux ne sont plus dédiés au support d'un seul type d'application, mais permettent de transférer à la fois de la voix, des données informatiques et des images vidéo (notion de réseau multimédia).

Un réseau peut être privé, propre à une organisation qui s'en réserve le droit exclusif d'utilisation, ou public. Dans ce cas, les services de télécommunication sont offerts à des personnes ou institutions différentes, selon certaines modalités d'abonnements.

Les principales technologies de transmission utilisées pour réaliser des réseaux grande distance sont les technologies TCP/IP, le relais de trames (*Frame Relay*) ainsi que ATM (*Asynchromous Transfer Mode*). Pour ce qui concerne le marché des réseaux locaux d'entreprise, la technologie prépondérante est fondée sur Ethernet et ses déclinaisons haut débit (*Fast Ethernet*, Ethernet commuté).

Dans le domaine des télécommunications, le transport optique et la technologie de commutation ATM ont marqué une étape dans l'évolution des infrastructures et des artères de transmission. Ils autorisent des transferts haut débit et de qualité, une allocation dynamique de bande passante, un débit variable et le multi-usage.

III.1.3 Eléments constitutifs des réseaux

III.1.3.1 Supports d'interconnexion

Pour relier des ordinateurs entre eux et les mettre en réseau, des supports de transmission sont nécessaires. Selon leur nature, on distingue les supports matériels (paires de fils torsadés, câbles coaxiaux, fibres optiques) des supports immatériels (faisceaux hertziens, ondes infra-rouges). Ces différents supports ont tous des caractéristiques spécifiques déterminant leur fiabilité et leur capacité à transmettre des quantités d'information plus ou moins importantes, à différentes vitesses.

Le débit autorisé sur un support d'interconnexion est la quantité d'informations transférée durant un laps de temps donné. Il s'exprime en kilo, méga, ou encore térabits par seconde (100 Mbit/s par exemple). Il est proportionnel à la bande passante du support de transmission (*bandwith*) qui exprime la plage de fréquences d'un signal que le support peut laisser passer sans modification.

---

22 L'organisation des liens d'interconnexion et la façon dont ils relient les éléments d'un réseau identifient sa topologie

23 Un réseau grande distance ou WAN (*Wide Area Network*) est un réseau reliant des ordinateurs répartis sur un territoire géographique plus ou moins vaste (supérieur à 100 km), voire mondial.

24 Un réseau est qualifié de local ou LAN (*Local Area Network*) lorsqu'il relie des ordinateurs dans un environnement géographique restreint à quelques kilomètres (une dizaine). Un réseau métropolitain ou MAN (*Metropolitan Area Network*) est un réseau d'interconnexion de réseaux locaux pouvant appartenir à des entités différentes et dont la couverture géographique n'excède pas 100 km. Une nouvelle terminologie est en passe d'émerger pour identifier les différents types de ressources mises en réseau ou encore pour distinguer un domaine d'application particulier. Ainsi, par exemple on trouve dans la littérature spécialisée les sigles suivants: HAN (*Home Area Network*), réseau interconnectant dans une maison des équipements télécommandables (four, vidéo, dispositifs lumineux et de chauffage, etc.), CAN (*Car Area Network*), SAN (*Storage Area Network*), etc.

III.1.3.2 Éléments de connectique

Le type de raccordement, ou élément de connectique à mettre en place entre un support de transmission et un ordinateur pour associer ces deux éléments, dépend du type de support et du mode de transmission utilisés. Ce boîtier de raccordement ou interface réseau, résout les problèmes de connectique et adapte le signal émis ou reçu par l'ordinateur au signal transmissible sur un support. Par exemple, *modem* (MOdulateur/DEModulateur) interface un ordinateur, qui est une machine digitale traitant des signaux numériques, avec un support de transmission tel qu'une ligne téléphonique analogique qui transmet des signaux sous forme continue[25]. Tout élément électronique est théoriquement connectable en réseau, s'il dispose d'une interface de raccordement matérielle et logicielle appropriée.

III.1.3.3 Machines spécialisées et serveurs d'information

Outre les systèmes des utilisateurs qui permettent d'accéder à un réseau et les ordinateurs dédiés à la gestion et au traitement des applications (machines hôtes ou *host* et serveurs d'informations), des ordinateurs de traitement des communications constituent l'infrastructure de transport d'un réseau. Ils assurent une ou plusieurs fonctions propres à la gestion et à la réalisation des télécommunications (optimisation et partage des ressources, acheminement des données, gestion des adresses, des noms, interconnexion, etc.). Ce sont, par exemple, des routeurs, multiplexeurs, concentrateurs, commutateurs ou des passerelles d'interconnexion.

Pour communiquer, il faut transmettre l'information de manière fiable selon des modalités d'échange satisfaisantes pour les correspondants. En effet, les systèmes interconnectés par les réseaux de télé-communication sont a priori différents. Pour qu'ils puissent dialoguer, ils doivent utiliser le même référentiel de communication, c'est-à-dire le même langage et respecter des règles d'échange communes.

Par analogie, deux individus de langue maternelle différente désirant s'échanger des informations se mettront d'accord sur la langue à employer. L'un fera peut-être l'effort de parler la langue de l'autre ou ils utiliseront une troisième langue connue des deux.

Si à cette conversation initiale s'intègre une tierce personne, puis une quatrième et une cinquième, etc. parlant d'autres langues, l'échange de données risque de devenir difficile à réaliser s'il faut traduire une langue dans une autre pour chaque paire d'interlocuteurs. Il est alors préférable de parler une langue commune et adoptée par l'ensemble des entités communicantes.

De manière similaire, les ordinateurs mis en réseau doivent respecter des protocoles de communication identiques et suivre les mêmes règles de dialogue afin de pouvoir communiquer. Ces protocoles sont intégrés dans des logiciels de communication. Ils permettent entre autres de réaliser l'acheminement correct des données et l'interfonctionnement des applications et des systèmes distants.

Des organismes reconnus par l'ensemble de la communauté industrielle définissent des normes internationales ou des standards de fait. L'ISO (*International Organization for Standardization*) et l'UIT (Union internationale des télécommunications) sont des organismes internationaux de normalisation qui proposent des normes internationales (normes de la série X.400 par exemple).

Une «norme de fait» est une norme non issue de ces organismes mais qui est largement adoptée par le marché. Elle devient alors une norme de référence, soit un standard de fait. Ainsi, tous les protocoles provenant de la communauté internet sont des standards de fait.

---

[25] L'information sortant d'un ordinateur, pour transiter sur un tel support, doit être modulée. L'information véhiculée sous forme analogique doit être à sa réception démodulée et présentée sous forme digitale à l'ordinateur destinataire. Un même dispositif, le modem, module et démodule l'information qui est émise et reçue par un ordinateur.

Les normes définissent, entre autres, la nature des services à offrir par les protocoles de communication et spécifient la façon de les réaliser. Cela permet la conception de solutions informatiques communicantes. Ainsi, grâce à l'utilisation des mêmes types de protocoles dans des machines différentes (ou hétérogènes), la communication entre elles est possible. L'universalité du réseau internet repose sur l'intégration des protocoles de la famille internet dans l'ensemble des machines reliées.

III.1.4 Infrastructure de télécommunication et autoroute de l'information

On appelle infrastructure de télécommunication l'ensemble des moyens de transmission à partir desquels des services de communication peuvent être développés. En effet, on dissocie les voies et les techniques d'acheminement des solutions et services de télécommunication offerts aux clients. Ainsi, par exemple, il est possible d'exploiter une infrastructure existante sans en être propriétaire et offrir à partir de cette facilité de transport des applications particulières.

La disponibilité d'équipements multimédias, d'infrastructures de communication performantes, ainsi que la convergence des mondes de l'audiovisuel, de l'informatique et des télécommunications, contribuent à réaliser la notion de chaîne d'information entièrement numérisée. Celle-ci représente la continuité numérique existante, tant au niveau de l'infrastructure de transport qu'au niveau du contenu, entre toutes les sources d'information et ses utilisateurs.

Le concept d'autoroute de l'information intègre la mise à disposition du grand public, via des infrastructures de communication performantes, d'un ensemble de services d'intérêt général ou de services marchands. Ils sont censés contribuer au bien-être des individus et peuvent être relatifs à la santé, l'éducation, la culture, l'aménagement du territoire, l'administration ou la presse, par exemple. De par la nature de certains services offerts via l'internet, ce média de communication peut être considéré comme une autoroute de l'information.

III.1.5 L'internet

III.1.5.1 Caractéristques générales

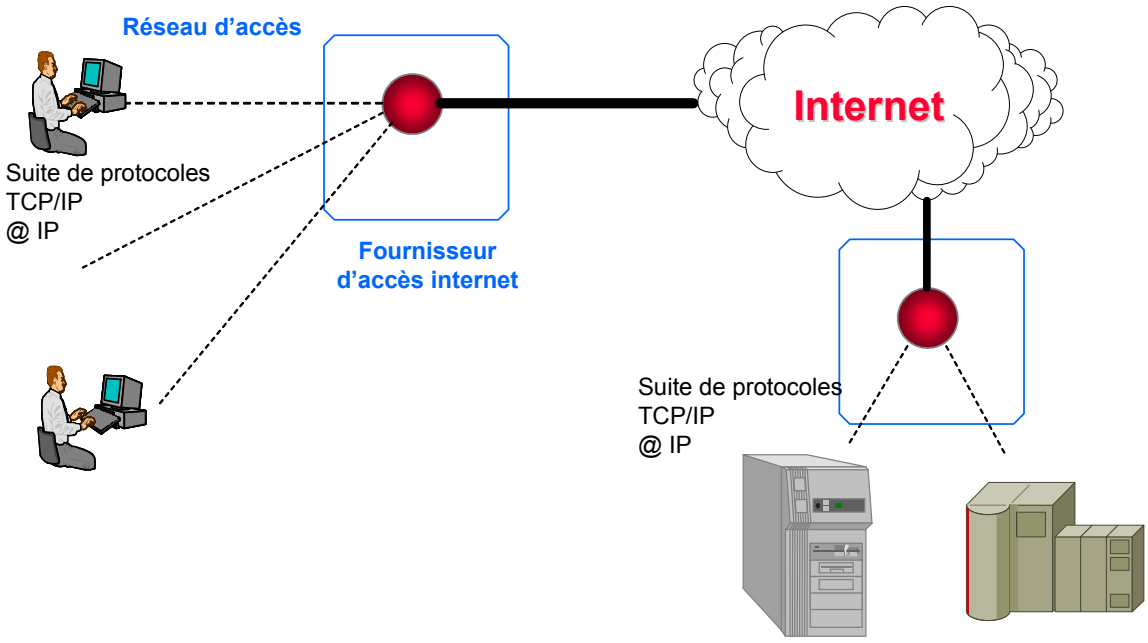
L'internet s'est déployé progressivement depuis les Etats-Unis, en reliant de proche en proche, des systèmes informatiques ainsi que des réseaux d'ordinateurs. Ce développement réticulaire se poursuit. Il détermine la structure du réseau qui est un réseau composés de réseaux. Il ne peut exister de contrôle global de l'ensemble des infrastructures mises ainsi bout à bout, dans la mesure où elles sont indépendantes et appartiennent à des organisations différentes.

Du point de vue matériel, l'internet, comme n'importe quel réseau de télécommunication ,est constitué de systèmes informatiques, d'éléments de connectique, et de supports de transmission. Parmi les systèmes informatiques, on distingue ceux qui permettent d'accéder au réseau et qui autorisent le dialogue avec l'utilisateur final (micro-ordinateur, téléphone portable, pager, agenda électronique, etc.), ceux qui supportent les applications (serveur web, serveur de bases de données, etc.) et ceux dédiés aux traitements «réseau» (routeurs, passerelles d'interconnexion, etc.).

L'échange de données entre ordinateurs s'effectue sur les supports de transmission qui les relient physiquement. Lorsque le point d'accès à l'infrastructure de l'internet s'effectue à partir d'un système autorisant la mobilité de l'utilisateur, comme le téléphone portable par exemple, on parle d'internet mobile.

Le transfert de données, leur acheminement ainsi que la communication entre processus informatiques répartis et utilisateurs humains, sont réalisés par des protocoles de communication de la famille TCP/IP[26]. Ces logiciels d'échange, normalisés dans le monde de l'internet, constituent une interface de communication qui permet l'interopérabilité de systèmes de nature différente. Pour communiquer dans l'environnement internet, un ordinateur doit posséder ces protocoles de communication ainsi qu'une adresse IP qui l'identifie de manière unique (Figure III.1).

Figure III.1 – Accès internet via un fournisseur d'accès, une suite de protocoles TCP/IP et une adresse IP

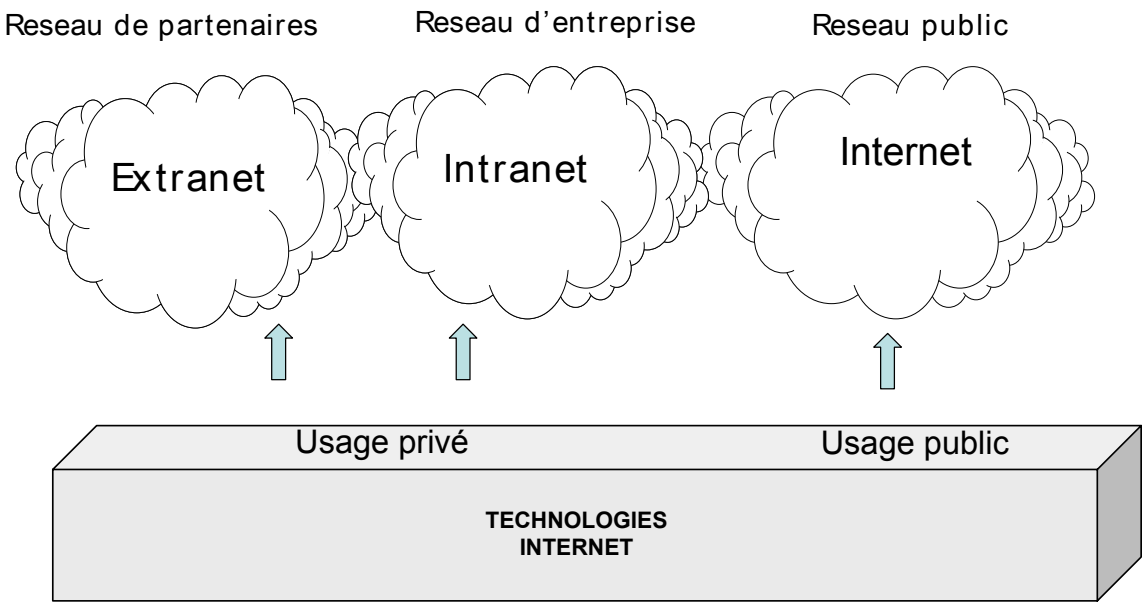


L'internet désigne l'ensemble de l'infrastructure de communication mise à disposition du public pour communiquer. Lorsqu'une organisation désire utiliser de manière privée et restrictive cette infrastructure, elle crée un réseau privé virtuel (VPN *Virtual Private Network*). Pour des besoins internes, elle peut aussi mettre en œuvre les technologies de l'internet et bâtir un réseau privé ou intranet. Lorsque l'intranet est également ouvert à un certain nombre de partenaires (clients, fournisseurs, etc.), il est qualifié *d'extranet* (Figure III.2).

Le web (*World Wide Web*) est, avec la messagerie électronique, l'application la plus importante de l'internet. A partir de la navigation web, une infinité de services a été développée. La navigation web est possible grâce, à un logiciel client, le navigateur (*browser*) implanté dans le poste de travail de l'utilisateur et qui permet d'accéder à distance à des serveurs web. Celui-ci permet de rechercher, consulter, transmettre des informations ou encore exécuter des programmes. La notion de surf ou de navigation sur le réseau provient du fait que les documents accessibles via l'application web sont des hyperdocuments. Cela signifie qu'ils ont été conçus, structurés et formatés de manière à en permettre une lecture non séquentielle, en fonction de balises et de liens déterminés à leur conception. En activant un lien, on accède à une autre partie de document ou à un autre document, situé ou non, sur un ordinateur distant. Ainsi on se déplace de site en site en activant ces hyperliens.

26 TCP/IP: Transmission Control Protocol/Internet Protocol.

Figure III.2 – Internet - Intranet - Extranet



III.1.5.2 Adresse IP et nom de domaine

On accède au réseau internet par l'intermédiaire de points d'accès gérés et contrôlés par des entreprises spécialisées dénommées fournisseur d'accès internet (ISP, pour *Internet Service Provider*). Chaque fournisseur d'accès est lui-même connecté au réseau internet par des lignes de télécommunication permanentes qu'il partage entre ses différents clients. Au-delà de ce service de base, il offre généralement un service de gestion de messagerie électronique et peut aussi héberger des sites web de ses clients.

Pour communiquer sur l'internet, il faut disposer d'une adresse internet (adresse IP). Il s'agit d'une suite binaire de 32 bits, identifiant sans ambiguïté chaque machine qui communique sur internet[27].

Une adresse IP est exprimée sous sa forme décimale, constituée par quatre nombres décimaux séparés par des points. Par exemple, l'adresse 128.10.2.30 correspond à la valeur binaire 10000000.00001010.00000010.00011110. Comme il est impossible de mémoriser des suites de nombres, même décimaux, on utilise des noms (plus ou moins mnémotechniques) ou adresses logiques, pour identifier les ressources de l'environnement internet. Ces adresses IP et ces noms correspondants sont stockés et gérés dans des annuaires électroniques dénommés serveurs de noms, dont l'implantation est connue sous le sigle DNS (*Domain Name Server*).

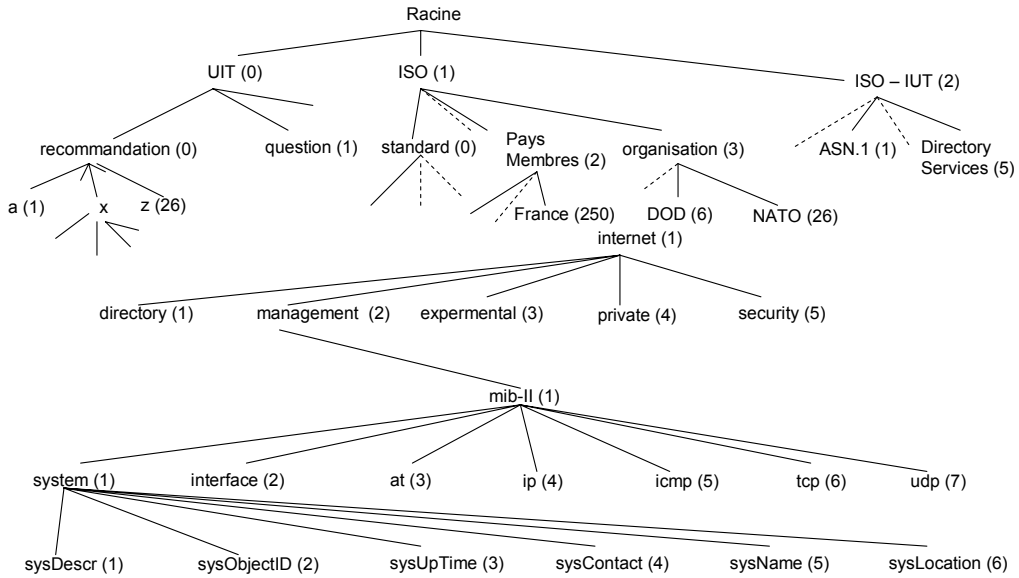
La mise en œuvre de communications dans un environnement ouvert nécessite de pouvoir attribuer un identificateur unique dans un domaine de dénomination déterminé. Il s'agit de pouvoir identifier les partenaires de la communication (adresses, systèmes, processus d'application, entités, objets de gestion, etc.) ainsi que les outils mis en œuvre pour les réaliser (protocoles). Pour assurer l'unicité des noms au niveau international, il existe des procédures d'enregistrement, auprès d'autorités compétentes, dont le rôle est d'attribuer un identificateur non ambigu et unique à l'objet que l'on désire identifier.

[27] L'adresse IP est unique; elle peut être alloué de manière permanente (adresse IP fixe) ou non (adresse IP temporaire).

La norme ISO 9834 a spécifié des autorités d'enregistrement et les a organisées selon une structure hiérarchique arborescente. De la racine de l'arbre partent trois branches aboutissant à des nœuds distincts de premier niveau qui représente le domaine de dénomination de l'UIT, de l'ISO, et d'un comité joint ISO-UIT qui constituent les autorités internationales d'enregistrement. Le niveau immédiatement inférieur à l'ISO autorise entre autres, l'enregistrement:

- des diverses normes ISO (0 standard);
- des membres de l'ISO (member-body 2) sous lequel on trouvera l'AFNOR (208), l'ANSI (310);
- des organisations (organization (3)) sous lequel dépendra par exemple le Département de la Défense américaine (DOD) (6) (Figure III.3).

Figure III.3 – Autorités et arbre d'enregistrement



Les noms de domaine génériques de l'internet sont enregistrés dans cette structure logique d'enregistrement. On ne s'intéresse alors qu'à la partie de l'arbre d'enregistrement dont le nœud constitue la racine des noms de domaines les plus élevés qualifiés de *top-level domains* (TLD). Ces derniers identifient principalement des pays indiqués par deux lettres (fr, it, uk, ch, nl, de, etc.) et des domaines fonctionnels comme:

- .com organisations commerciales;
- .edu institutions académiques d'Amérique du Nord;
- .org organisations, institutionnelles ou non;
- .gov gouvernement américain;
- .mil organisations militaires américaines;
- .net opérateurs de réseaux;
- .int entités internationales;
- .biz pour ce qui concerne le monde des affaires;
- .info pour tous les usages;
- .name pour les individus;

- .museum pour les établissements dans lesquels sont rassemblées et classées des collections d'objets, en vue de leur conservation et de leur présentation au public;
- .aero pour l'industrie air – transport;
- .coop pour les coopératives;
- .pro pour les professions.

À l'intérieur de ces grands domaines de désignation, se trouvent des sous-domaines, qui correspondent à de grandes entreprises ou à d'importantes institutions.

L'IANA (*Internet Assigned Number Authority*)[28] basé à l'ICANN (*Internet Corporation For Assigned Names and Numbers*)[29] est responsable de l'attribution des noms et adresses et doit s'assurer de leur unicité. Cette responsabilité de gestion des noms peut-être déléguée à un sous-domaine qui est, d'un point de vue hiérarchique, sous son autorité.

Enregistrer un nom de domaine consiste à insérer une entrée dans un annuaire de désignations. Cela revient à créer un nouvel arc dans l'arbre d'enregistrement géré par une organisation habilitée. Il en existe plusieurs au niveau international, notamment pour ce qui concerne les domaines.biz,.com,.info, .name,.net,.org.

Pour la France, par exemple, l'AFNIC[30] est l'autorité d'enregistrement accréditée (*Accredited Registrar Directory*) par l'ICANN (*Internet Corporation for Assigned Names and Numbers*).

C'est une association américaine – sur territoire américain, opérant selon la législation américaine – qui possède le pouvoir de l'attribution et la gestion des adresses[31]. Elle contrôle ainsi l'accès à l'internet. Ceci pose un réel problème de dépendance des organisations et des Etats vis-à-vis d'une supra-structure étrangère qui se veut ouverte sur le reste du monde mais dont le poids des représentants non américains est faible.

Le critère de sécurité relatif à la disponibilité (des infrastructures, services, données) qui passe par l'accessibilité au réseau internet ne peut être ni contrôlé, ni maîtrisé par les organisations. Elles sont tributaires pour leur accès à l'internet, de l'attribution des adresses IP et des noms de domaine, d'entités qui leurs sont externes.

Les annuaires d'enregistrement des noms de domaine peuvent être vus comme des bases de données gérées par des serveurs DNS. Une quinzaines de serveurs racine DNS (*root servers*) sont coordonnés par l'ICANN, la grande majorité des serveurs racine se situe sur le territoire nord américain. Ils gèrent les noms de domaine et les adresses IP de plus haut niveau (*top-levels domains*). Cela comprend l'ensemble des domaines précédemment cités (.org,.com, etc.) et aussi les 244 noms de domaine des différents pays (.cn (Chine),.ga (Gabon),.lk (Sri Lanka),.pf (Polynésie française), etc.). Des serveurs DNS locaux dits de résolution (*resolvers*) possèdent une copie des informations contenues dans les serveurs racine. Souvent associés à des points stratégiques d'accès au réseau ou liés à des fournisseurs d'accès internet (*Internet Service Providers* – ISP), ils permettent de répondre aux requêtes des utilisateurs relatives à la traduction d'un nom de domaine en une adresse IP (Figure III.4)[32].

---

28 IANA: www.iana.org/

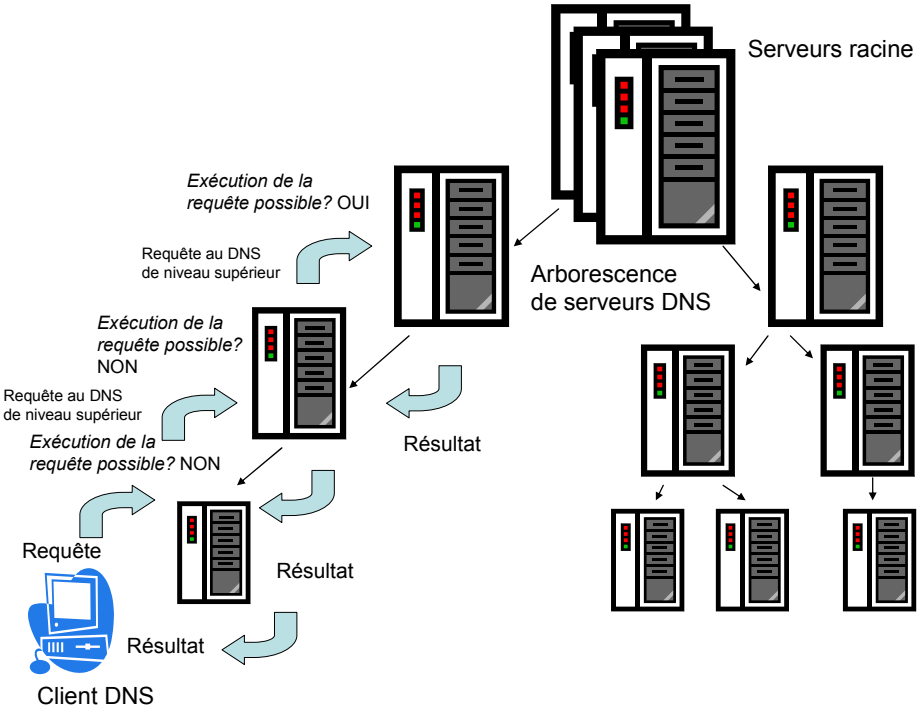
29 ICANN: www.icann.org/index.html

30 AFNIC: www.nic.fr

31 Selon l'ICANN: «*…The Internet Corporation for Assigned Names and Numbers (ICANN) is an internationally organized, non-profit corporation that has responsibility for Internet Protocol (IP) address space allocation, protocol identifier assignment, generic (gTLD) and country code (ccTLD) Top-Level Domain name system management, and root server system management functions. These services were originally performed under U.S. Government contract by the Internet Assigned Numbers Authority (IANA) and other entities. ICANN now performs the IANA function* ».

32 Figure issue du livre «Sécurité informatique et télécoms: cours et exercices corrigés»; S. Ghernaouti-Hélie; Dunod 2006.

Figure III.4 – Arborescence de serveurs DNS



Il est primordial que les adresses, les processus, les systèmes impliqués dans la gestion des noms et adresses, dans l'acheminement des donnés soient disponibles, intègres, fiables et sécurisés. Il est de la responsabilité des entités en charge des infrastructures de transport de protéger et de gérer efficacement leurs environnements de communication.

III.1.5.3 Protocole IPv4

La version 4 du protocole internet (IPv4)[33] qui existe depuis l'origine du réseau internet, est encore largement utilisée. Ce protocole a pour rôle d'encapsuler (d'envelopper) les données à transmettre pour constituer des paquets IP qui seront acheminés à travers le réseau internet jusqu'à leur destination. Chaque paquet contient entre autres, l'adresse IP source du système émetteur et l'adresse IP du système de destination.

L'acheminement se réalise de proche en proche à chaque système intermédiaire (routeur) traversé selon l'interprétation des adresses des paquets et l'algorithme de routage des routeurs.

Le protocole IPv4 n'intègre aucune fonction, aucun mécanisme permettant d'offrir un service de sécurité. En effet, IPv4 ne permet pas d'effectuer l'authentification de la source ou de la destination d'un paquet, ni la confidentialité des données qu'il transporte, ni la confidentialité des adresses IP impliquées lors d'un transfert d'informations entre deux entités. De plus, le protocole s'effectuant en mode sans connexion, ne garantit pas:

- la remise des données (perte possible de données);
- la livraison de données au bon destinataire;
- l'ordonnancement (séquencement) correcte des données.

---

33 IPv4: RFC 0791 –www.ietf.org/rfc/rfc0791.txt IPv4 et principaux protocoles de la suite TCP/IP: TCP: RFC 0793 – www.ietf.org/rfc/rfc0793.txt – UDP: RFC 0768 – www.ietf.org/rfc/rfc0768.txt – FTP: RFC 0959 – www.ietf.org/rfc/rfc0959.txt – HTTP version 1.1: RFC 2616 – www.ietf.org/rfc/rfc2616.txt – Telnet: RFC 0854 – www.ietf.org/rfc/rfc0854.txt

Le protocole IP de niveau 3 de l'architecture OSI, offre un service non fiable de remise de paquets IP. Il fonctionne en mode dit de «*best effort*», c'est-à-dire qu'il fait au mieux en fonction du contexte et la livraison de paquets n'est pas garantie. En fait, aucune qualité de service ne l'est et il n'y a donc pas de reprise sur erreur. Ainsi un paquet peut être perdu, modifié, dupliqué, fabriqué (forgé) ou remis hors séquence sans que l'émetteur ou le destinataire en soit informé. Le fait qu'une liaison logique ne soit pas préalablement établie entre un émetteur et un destinataire, signifie que l'émetteur envoie ses paquets sans en avertir le destinataire et qu'ils peuvent se perdre, prendre des routes différentes, ou arriver dans le désordre.

La prise en compte de ce manque de qualité de service a conduit à implanter dans les systèmes d'extrémité le protocole TCP (Transmission Control Protocol) qui offre un service de transport fiable en mode connecté (niveau 4 de l'architecture OSI). Le protocole TCP n'offre pas de service de sécurité à proprement parler.

Chapitre III.2 – Outils de la sécurité

Assurer la sécurité des informations, des services, des systèmes et des réseaux consiste à réaliser la disponibilité, l'intégrité, la confidentialité des ressources ainsi que la non-répudiation de certaines actions, ou l'authenticité d'évènements ou de ressources.

La sécurité des informations n'a de sens que si elle s'applique sur des données et des processus dont on est sûr de l'exactitude (notion de qualité des données et des processus) afin qu'ils soient pérennes dans le temps (notion de pérennité des données et de continuité des services).

Les principales solutions de sécurité se basent sur la mise en œuvre de techniques de chiffrement, d'isolation d'environnements, sur la redondance des ressources, sur des procédures de surveillance, de contrôle, de gestion des incidents, de maintenance, de contrôle d'accès ou de gestion de systèmes.

La sécurité informatique et des télécoms est obtenue par une succession de barrières (les mesures de protection) qui augmentent le niveau de difficulté que de potentiels attaquants doivent franchir pour accéder aux ressources. Elles ne solutionnent pas un problème de sécurité, elles le déplacent et font porter la responsabilité de la sécurité sur d'autres entités. Les solutions de sécurité ont besoin d'être protégées et sécurisées afin qu'elles puissent offrir un certain niveau de sécurité (récursivité de la sécurité).

III.2.1 Chiffrement des données.

La mise en œuvre de techniques de chiffrement permet de réaliser la confidentialité des données, de vérifier leur intégrité et d'authentifier des entités.

Il existe deux grands types de système de chiffrement de données: le chiffrement symétrique (à clé secrète) et le chiffrement asymétrique (à clé publique).

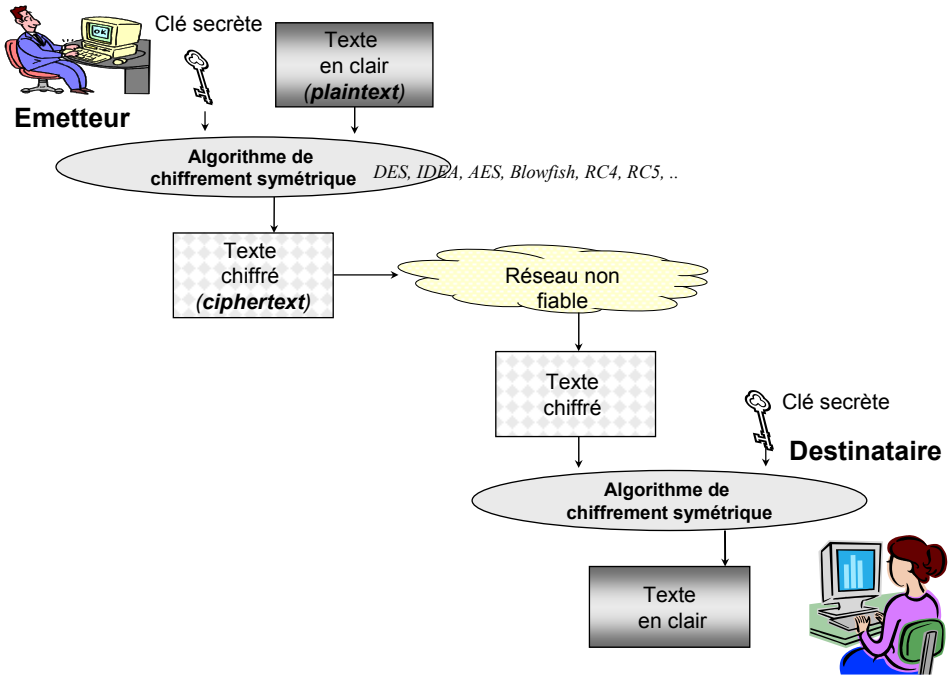
Divers algorithmes de chiffrement existent. Quel que soit leur mode opératoire (symétrique ou asymétrique), ils reposent sur l'usage de clés. Généralement leur degré de robustesse est lié à la capacité à gérer les clés de chiffrement de manière sécurisée, à la longueur de la clé (la longueur minimale de la clé est fonction du type d'algorithme), de la sécurité de la plateforme matérielle et logicielle dans laquelle les algorithmes de chiffrement sont implantés et s'exécutent.

III.2.1.1 Chiffrement symétrique

Pour chiffrer ou déchiffrer un texte, il faut détenir une clé et à un algorithme de chiffrement. S'il s'agit de la même clé pour effectuer ces deux opérations, le système de chiffrement est qualifié de symétrique. L'émetteur et le récepteur doivent posséder et utiliser la même clé secrète pour rendre confidentielles des données et pour pouvoir les comprendre, ceci qui pose le problème de la gestion et de la diffusion des clés secrètes (Figure III.5).

Les principaux algorithmes de chiffrement symétriques sont: DES, RC2, RC4, RC5, IDEA et AES[34].

Figure III.5 – Le chiffrement symétrique



III.2.1.2 Chiffrement asymétrique ou à clé publique

Un système de chiffrement asymétrique est basé sur l'usage d'un couple unique de deux clés, calculées l'une par rapport à l'autre. Cette bi-clé est constituée d'une clé publique et d'une clé privée. Seule la clé dite publique peut être connue de tous, tandis que la clé privée doit être confidentielle et traitée comme un secret.

L'émetteur chiffre un message avec la clé publique du destinataire du message et le destinataire le déchiffre avec sa clé privée (Figure III.6).

Les principaux algorithmes de chiffrement à clé publique, dont le nom est celui de leurs inventeurs, utilisent le plus souvent des clés de longueur variant de 512 à 1024 bits, voire 2048 bits. Les principaux algorithmes de chiffrement sont les algorithmes: RSA[35] (pour R. Rivest, A. Shamir, L. Adelman), Diffie-Hellman[36], El Gamal[37].

III.2.1.3 Clés de chiffrement

Une clé de chiffrement est le secret du secret. Les clés secrètes des systèmes de chiffrement, doivent être gérées de manière confidentielle.

---

34 Références:

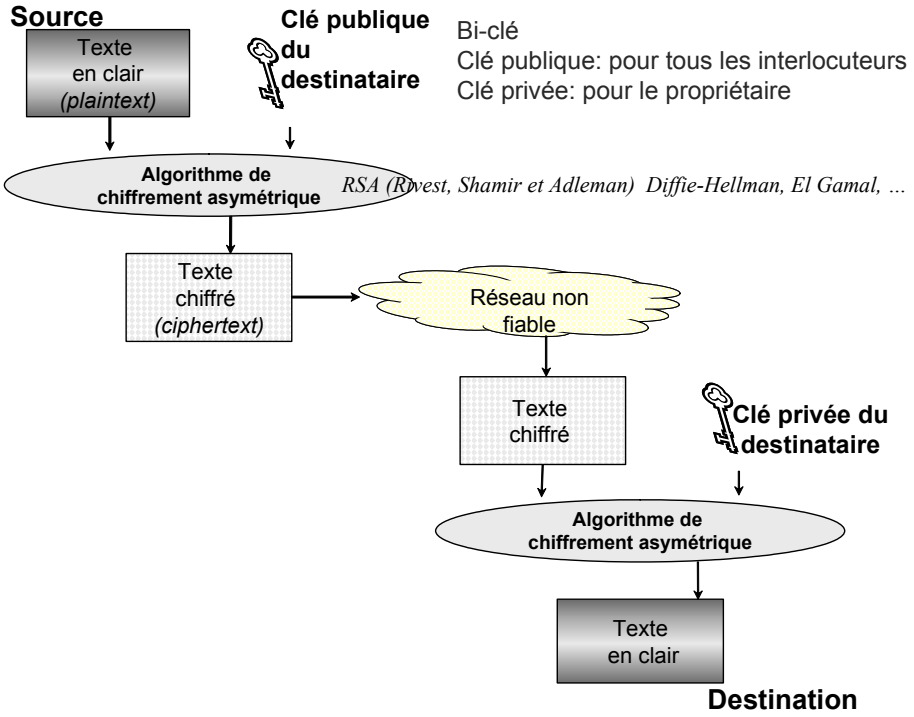
35 RSA: Schneier B, «Applied cryptography» 1996. Deuxième edition 1996.

36 Diffie-Hellman: www.ietf.org/rfc/rfc2631.txt

37 El Gamal: Schneier B, «Applied cryptography» 1996. Deuxième edition 1996.

La sécurité du processus de chiffrement, repose en grande partie sur la confidentialité et la longueur des clés utilisées, sur la robustesse des algorithmes et sur la sécurité des plates-formes matérielles et logicielles qui les supportent.

Figure III.6 – Le chiffrement asymétrique



III.2.1.4 Infrastructure de gestion de clés

Une infrastructure de gestion de clés – IGC, (PKI – *Public Key Infrastructure*) permet de mettre en œuvre des systèmes de chiffrement asymétrique. Les principales fonctions supportées sont:

- la génération d'un couple unique de clés (clé privée – clé publique), son attribution à une entité et la sauvegarde des informations nécessaires à sa gestion, archivage des clés, procédures de recouvrement en cas de perte par l'utilisateur ou de demande de mise à disposition par les autorités judiciaires;
- la gestion des certificats numériques, création, signature, émission, validation, révocation, renouvellement des certificats;
- la diffusion des clés publiques aux ressources qui la solliciteraient et qui seraient habilitées à l'obtenir;
- la certification des clés publiques (signature des certificats numériques).

III.2.1.5 Certificat numérique

Un certificat numérique constitue, la carte d'identité numérique d'une entité (personne morale ou physique) ou d'une ressource informatique à qui il appartient. Il contient, entre autres, l'identification de son propriétaire, la clé publique qui lui est attribuée ainsi que l'identification de l'organisme qui l'a délivré.

La norme X.509 «*Directory authentification framework*» propose un cadre architectural pour la réalisation d'un service d'authentification basé sur l'usage de certificats numériques et spécifie la structure et le format d'un certificat numérique. Cette structure normalisée est à la base de nombreuses solutions du marché (Figure III.7).

Figure III.7 – Principaux paramètres d'un certificat numérique selon la norme X.509v3

Version du certificat
Numéro de série
Algorithme utilisé pour signer le certificat
Nom de l'organisme qui a généré le certificat Le couple numéro de série / nom de l'organisme doit être unique
Période de validité
Nom du propriétaire du certificat
Clé publique du propriétaire
Informations additionnelles concernant le propriétaire ou les mécanismes de chiffrement
Signature du certificat Algorithme et paramètres utilisés pour la signature et signature à proprement parlé

Pour valider le certificat reçu, le client doit obtenir la clé publique de l'organisme qui a créé le certificat relatif à l'algorithme utilisé pour signer le certificat et déchiffrer la signature contenue. A l'aide de ces informations, il calcule la valeur du condensé (résumé ou *hash*) et compare la valeur trouvée avec celle contenue dans le dernier champ du certificat, si les deux valeurs correspondent, le certificat est authentifié. Ensuite, il s'assure que la période de validité du certificat est correcte.

Le contrôle d'accès basé sur les certificats numériques permet la connexion d'un nombre important d'utilisateurs à un serveur donné. Le contrôle est basé sur les informations contenues dans le certificat numérique du client. Le serveur fait alors confiance à la véracité des certificats et à la façon dont ils sont émis, ce qui constitue une brèche dans la sécurité des systèmes, vu qu'il est possible de corrompre un serveur de certification ou même de créer un certificat numérique falsifié. En outre, le contrôle de validité d'un certificat est difficile à réaliser. En effet, la révocation des certificats reste une tâche très ardue puisque l'information doit être transmise à tous les partenaires et inscrite dans le CRL (*Certificate Revocation List*). Cette révocation doit être réalisée dès qu'un changement dans le contenu d'un certificat survient (lorsque par exemple les informations du certificat deviennent obsolètes, la clé privée de l'utilisateur a été corrompue, l'utilisateur ne fait plus partie de l'entreprise, etc.). La consultation systématique de cette base de données accentue la lourdeur du contrôle d'accès et réduit la disponibilité des serveurs même pour les utilisateurs autorisés.

III.2.1.6 Tiers de confiance

Quelle que soit son appellation, tiers de confiance, autorité d'enregistrement ou autorité de certification, l'organisme qui met en place une infrastructure à clé publique, a pour fonction principale de produire des certificats établissant la valeur de la clé publique, attribuée à une entité (notion de certificats clients).

Un client, émet une demande d'enregistrement (demande de certification) auprès d'une Autorité de certification (inscription du client via un service web). Des preuves de l'identité du client peuvent être demandées par le serveur d'enregistrement selon les procédures d'identification et d'authentification mises en place par l'autorité. Après validation des données, le serveur de certification génère les clés de chiffrement et construit un certificat numérique au nom du client, signe avec sa clé privée le certificat (certification du certificat numérique) et envoie le certificat au client. Ce dernier utilisera la clé publique de l'autorité pour s'assurer que le certificat est bien produit par l'autorité en question.

Une Autorité de certification est un tiers de confiance qui délivre des certificats numériques et qui permet de vérifier la véracité de certaines informations.

III.2.1.7 Inconvénients et limites des infrastructures de gestion de clés

La multiplicité des autorités de certification pose le problème de leur reconnaissance mutuelle, de leur interopérabilité, de la compatibilité des certificats et du champ de leur validité. Toutefois, il n'est pas souhaitable de ne disposer que d'une seule autorité mondiale de certification, du fait du pouvoir étendu et excessif qui lui serait de facto conféré, et du fait de l'importance de l'infrastructure à mettre en place. Il existe un réel manque de confiance des utilisateurs dans les autorités de certification qui sont le plus souvent étrangères (valeur des certificats? garantie de sécurité? protection des données personnelles?, etc.).

Les limites inhérentes aux infrastructures de gestion de clés résident dans:

- la complexité, le coût du déploiement et de la gestion d'une infrastructure;
- le haut niveau de sécurité nécessaire à la réalisation des services des infrastructures de gestion de clés;
- la validité, la durée de vie, la résiliation des certificats.

Parmi les points relatifs à la mise en œuvre de services offerts par une infrastructure de gestion de clés qui peuvent poser problème, retenons:

- Problème politique: la majorité des infrastructures PKI – Autorités de certification, appartient à des entités américaines (USA). Cela soulève la question de la performance et la question de la confiance dans ces entités qui du fait des services offerts: création, sauvegarde, distribution des clés privées et publiques, des données d'identification, notarisation des évènements; du manque de garantie de l'usage non abusif des données, de la neutralité dans les échanges, de moyens de recourt en cas de litige avec l'autorité de certification;
- Problème technologique: les systèmes de chiffrement classiques peuvent être cassés, certains certificats numériques n'ont aucune valeur sécuritaire et ne garantissent rien, des fraudes sont possibles, la sécurité des infrastructures est assurées par des moyens classiques de sécurité qui peuvent être contournés. De plus, l'usage d'une infrastructure de gestion de clés déplace le problème de la sécurité des échanges mais ne le résout pas à proprement parler.
- Problème organisationnel: interopérabilité des infrastructures, déploiement, gestion, maintenance, sécurité, complexité, etc.

III.2.1.8 Signature et authentification

Un émetteur chiffre avec sa clé privée un message. Toute entité connaissant la clé publique de cet émetteur déchiffrera le message, ce qui validera le fait qu'il a bien été créé à l'aide de la clé privée correspondante.

Un document peut être signé électroniquement (notion de signature numérique) via un algorithme de chiffrement à clé publique. Les actions suivantes sont alors réalisées:

- création d'un message de déclaration d'identité qui est la signature (ex. «Je m'appelle Alpha Tango Charlie») qui est chiffrée avec la clé privée de l'émetteur et associée au message à transmettre;
- le message et sa signature sont chiffrés avec la clé publique du destinataire et transmis;
- le destinataire déchiffre le message avec sa clé privée et détache la signature qu'il déchiffre avec la clé publique de l'émetteur.

Attention, rien n'empêche de réutiliser la signature numérique d'un message en lieu et place de l'émetteur réel, on peut également constituer une signature numérique à la place d'un partenaire après lui avoir volé sa clé privée….Pour augmenter le niveau de sécurité de la signature numérique, celle-ci est construite à partir du contenu du message ce qui permet de réaliser l'intégrité et l'authentification de l'émetteur d'un message.

III.2.1.9 Intégrité des données

Vérifier que les données n'ont pas été modifiées lors de leur transfert est possible en y associant un résumé (condensé) qui est émis en même tant que les données. Celui-ci est le résultat d'une fonction de calcul appliquée aux données. Le destinataire recalcule avec la même fonction la valeur du résumé à partir de données reçues. Si la valeur obtenue diffère, il en déduit que les données ont été modifiées. Le résumé peut être lui-même chiffré avant que les données ne soient émises ou stockées.

L'un comme l'autre, les systèmes de chiffrement à clé symétrique ou asymétrique permettent de savoir si des données transmises ont été modifiées, car leur déchiffrement devient alors impossible. Cela contribue à réaliser un contrôle d'intégrité, mais ne permet pas de s'assurer que des données n'ont pas été complètement détruites.

Pour un contrôle d'intégrité plus performant, on applique au message original une fonction le transformant en une petite suite aléatoire de bits qui constitue en quelque sorte son empreinte digitale (*digest – résumé – condensé*).

Une fonction dite fonction *digest* (ou *one-way hash function*), génère un message *digest*, c'est-à-dire son empreinte digitale, plus courte que le message original et incompréhensible. Celle-ci est ensuite chiffrée avec la clé privée de l'émetteur et associée au message à transmettre. Sur réception du message et de son empreinte, le destinataire déchiffre cette dernière avec la clé publique de l'émetteur puis, recalcule à partir du message reçu avec la même fonction *hash*, l'empreinte et la compare ensuite avec celle reçue. Si le résultat est identique, le destinataire a ainsi vérifié l'identité de l'émetteur et est assuré de l'intégrité du message. En effet, si le message est altéré, même légèrement, son empreinte est alors considérablement modifiée.

Par une utilisation conjointe des techniques de chiffrement, de signature et d'empreinte digitales, on peut estampiller les messages pour garantir l'intégrité des données. Ces procédures sont consommatrices de temps processeur et ralentissent de façon non négligeable les performances d'un environnement d'exécution.

III.2.1.10 Non-répudiation

Le service de non-répudiation consiste à prévenir le refus, le démenti qu'un message ait été émis ou reçu ou qu'une action, transaction ait eu lieu. Cela permet de prouver par exemple qu'une entité est liée à une action ou à un événement.

La non-répudiation est basée sur une signature unique ou sur une identification qui prouve qui a créé le message. Pour assurer ce service, on peut faire appel à un algorithme de chiffrement à clé publique. On peut également avoir recours à un tiers de confiance pour lui faire jouer un rôle de cybernotaire.

III.2.1.11 Limites des solutions de sécurité basées sur le chiffrement

La confiance envers les solutions de chiffrement commercialisées ne peut être que toute relative, dans la mesure ou aucune garantie, aucun moyen de vérification ne sont offerts (existence de portes dérobées (*back door*) dans les logiciels?, clés secrètes dupliquées, divulguées? ect.). Par ailleurs, aucune preuve n'est donnée quand au fait que les algorithmes actuellement réputés fiables le seront encore dans un futur proche.

III.2.2 Protocole IP sécurisé

La prise en compte des besoins de sécurité ont conduit à la révision de la version 4 du protocole internet. C'est également afin de pouvoir, d'une part, disposer d'une plage d'adresses plus importante et augmenter le nombre d'adresses internet disponibles et d'autre part, pour pouvoir faire une allocation dynamique de bande passante pour supporter des applications multimédias, que le protocole IP a fait l'objet d'une refonte connue sous le nom d'IPnG (*Internet Protocol next Generation*) ou IP version 6 (IPv6)[38].

III.2.2.1 Protocole IPv6

En 1994[39] l'IAB (*Internet Activity Board*)[40].adressait les besoins de sécurité du protocole IP. La version 6 du protocole IP (IPv6) inclut des facilités d'authentification et de confidentialité.

Les principales évolutions d'IPv6 par rapport à IPv4 portent sur les points suivants [RFC 2460]:

- le support d'un adressage étendu et hiérarchisé; les adresses sont codées sur 128 bits (16 octets) et non plus sur 32 bits (4 octets); la représentation des adresses s'effectue en nombres hexadécimaux[41] séparés par des deux points tous les 2 octets et non plus en notation décimale pointée; (exemple: 0123:4567:89ab:cdef:0123:4567:89ab:cdef);
- la possibilité de pouvoir faire de l'allocation dynamique de bande passante pour le support d'applications multimédias;
- la capacité à créer des réseaux IP virtuels;
- le support de procédures d'authentification et de chiffrement, via des en-tête à options;
- la simplification des en-têtes des paquets afin de faciliter et accélérer le routage.

L'adoption d'IPv6 impose entre autres, la modification du schéma d'adressage, de gestion des adresses[42], la mise en place dans tout l'environnement internet de systèmes supportant IPv6, des systèmes fonctionnant avec les deux versions, la synchronisation à grande échelle de la migration des versions, etc.

Pour toutes ces raisons, la version 6 spécifiée en 1995 n'est actuellement toujours pas largement implantée et aucune incitation gouvernementale ou recommandation internationale ne semble pouvoir imposer l'adoption de la version 6 du protocole sur l'ensemble du réseau. Seules quelques infrastructures privées intègrent IPv6.

La mise en œuvre du nouveau protocole internet (IPv6) intégrant en natif des fonctions de sécurité n'est pas courante, aussi, pour répondre aux besoins de sécurité du réseau, une solution intermédiaire dénommée IPSec[43], compatible avec IPv6 et IPv4, a été développée et adoptée par la communauté internet. L'IETF (*Internet Engineering Task Force*)[44] a établi en 1995 plusieurs documents (RFC 1825 à 1829) spécifiant les manières de sécuriser une infrastructure internet.

---

38 IPv6: RFC 1883 en 1995, remplacée en décembre 1998 par la RFC 2460 – www.ietf.org/rfc/rfc2460.txt

39 RFC 1636: Report of IAB Workshop on Security in the Internet Architecture. February 8-10, 1994.

40 www.iab.org/

41 Alphabet d'un système de numération hexadécimal (base 16): 0 1 2 3 4 5 6 7 8 9 A B C D E F

42 RFC 1886 a identifiée en 1995 les modifications a effectuer dans les DNS pour supporter IPv6.

43 RFC 2401 – www.ietf.org/rfc/rfc2401.txt

44 IETF: www.ietf.org

III.2.2.2 Protocole IPSec

IPSec permet de rendre confidentiel le contenu des paquets véhiculés par le protocole. IPSec propose des services de confidentialité et d'authentification des données au niveau de leur transfert par le protocole IP, via l'implantation de l'en-tête d'extension d'authentification (*Authentication Header* [AH]) ou de l'en-tête de confidentialité – authentification (*Encapsulating Security Payload Header* [ESP]).

Chaque application, quelle que soit la nature du trafic qu'elle génère, peut utiliser ces services de sécurité sans être modifiée. IPSec fonctionne en mode point à point (on sécurise les données entre un émetteur et un récepteur via une association de sécurité).

L'en-tête d'authentification (AH) offre des services d'authentification et d'intégrité des paquets IP. Cela permet de garantir que les données n'ont pas pu être modifiées lors de leur transfert et que l'adresse source est bien celle qui figure sur le paquet.

L'en-tête d'*Encapsulating Security Payload* (ESP) permet la réalisation de mécanismes de chiffrement (chiffrement symétrique comme DES, Triple DES, RC5 ou IDEA) et propose des services d'authentification similaires à ceux proposés par l'*Authentication Header* (AH).

Les algorithmes de chiffrement utilisent des clés qui sont à générer et à diffuser. La gestion des clés de chiffrement est donc une tâche importante à réaliser lors de la mise en œuvre de solutions basées sur IPSec. Parmi les protocoles d'échange de clés citons: *Oakley Key Determination protocol*[45] est basé sur l'algorithme d'échange de clés Diffie-Hellman [RFC 2412]; ISAKMP (*Internet Security Association and Key Management Protocol*) [RFC 2408]; IKE (*Internet Key Exchange*) [RFC 2409].

III.2.2.3 Réseaux privés virtuels

L'implantation du protocole IPSec au niveau des points d'accès au réseau internet permet de créer entre ces points, un canal de communication dont les extrémités sont authentifiées (Figure IIII.8).

Ces extrémités se trouvent dans des systèmes de l'organisation et donc physiquement protégées. Selon l'option retenue, les données véhiculées sur cette connexion pourront être chiffrées. Ainsi on sait établir un chemin sécurisé entre deux points d'une infrastructure de réseau non fiable (notion de réseau privé virtuel). Notons que le terme «réseau» dans l'expression «réseau privé virtuel» est abusif puisque seule une connexion logique (virtuelle) est crée.

III.2.3 Sécurité des applications

La plus part des applications possèdent une version sécurisée qui permet le plus souvent de réaliser l'authentification des correspondants et le chiffrement des données transmises.

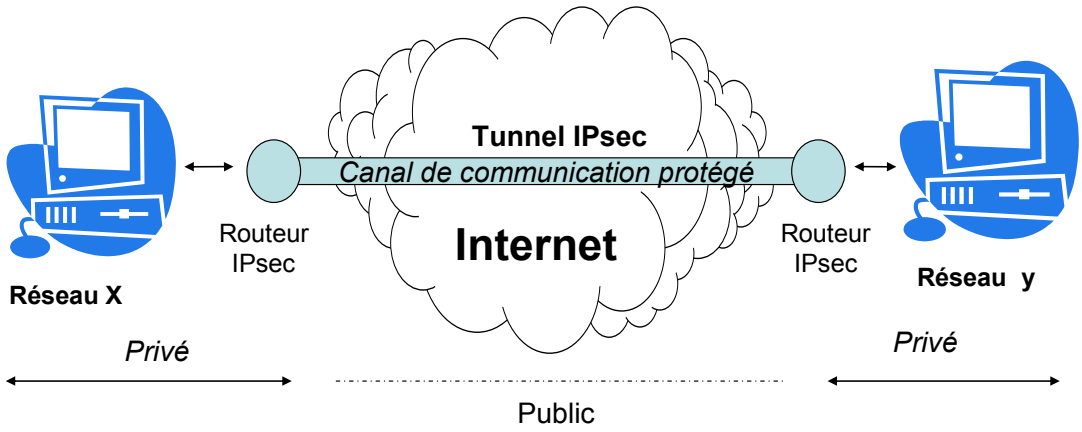
Une alternative à l'implantation de nouvelles versions sécurisées des protocoles d'application, consiste à implanter un mécanisme commun de sécurité, offrant des services génériques de sécurité à toutes les applications. Le logiciel SSL (*Secure Sockets Layer*) est couramment utilisé à l'heure actuelle, notamment pour réaliser des transactions commerciales sur l'internet.

L'usage extensif de documents hypertextes comme le téléchargement de contenus actifs ou non posent de nombreux problèmes de sécurité concernant entre autre: leur origine, leur auteur, leu authenticité, leur caractère nuisible ou non, etc. Des éléments de réponses à cette nouvelle dimension de la sécurité des systèmes d'information, commencent à émerger: techniques de signature de documents XML, de tatouage, de gestion des droits électroniques, afin de conférer à la sécurité une certaines persistance. Un niveau donné de sécurité doit pouvoir être conservé, même si l'objet concerné par la sécurité, sort des frontières physiques de l'environnement dans lequel sa sécurité est habituellement gérée.

---

45 Oakley Key determination protocol: RFC 2412 – www.ietf.org/rfc/rfc2412.txt

Figure III.8 – Constitution d'un réseau privé virtuel par un canal de communication IPsec



III.2.4 Protocoles de sécurité SSL (Secure Sockets Layer) et S-HTTP (Secure HTTP)

SSL (*Secure Sockets Layer*) est un logiciel assurant la sécurité des échanges applicatifs, qui est d'ailleurs supporté par la majorité des navigateurs web du marché.

Les deux entités communicantes d'une connexion SSL s'authentifient en faisant appel à une procédure de certification et à un tiers de confiance. Elles négocient ensuite le niveau de sécurité à appliquer au transfert. Les données transmises sont alors chiffrées pour cette communication via SSL (Figure III.8).

L'implantation de SSL a un fort impact du côté du serveur du fait de la nécessaire certification. Cela implique un dialogue avec une autorité de certification reconnue et demande également que les relais applicatifs des *firewalls* supportent le mode de fonctionnement de SSL. La certification est parfois considérée comme un frein au déploiement de cette solution.

L'extension au protocole HTTP (*Secure* HTTP, S-HTTP) est une solution alternative développée par l'association CommerceNet. S-HTTP offre les mêmes facilités de sécurité que SSL, avec les mêmes contraintes de certification, mais ne supporte que les flux de données du protocole HTTP. Cette solution est peu adoptée.

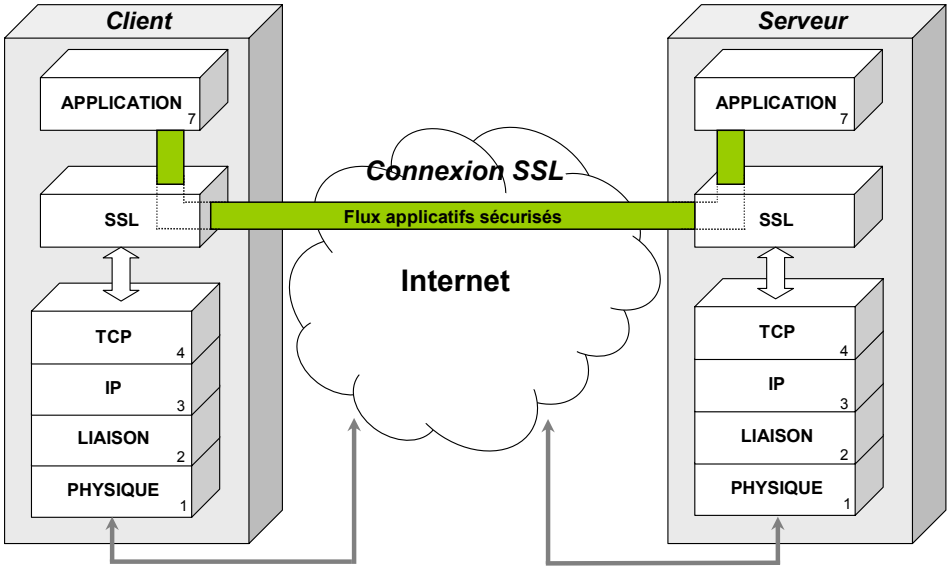
III.2.5 Sécurité de la messagerie électronique et des serveurs de noms

Les risques de sécurité encourus, relatifs à l'usage d'un système de messagerie, sont liés à:

- la perte, l'interception, l'altération, la destruction de messages;
- l'infection des systèmes par le biais de messages contenant des virus, vers ou cheval de Troie;
- l'harcèlement: inondation de messages, junk mail, messages non sollicités (spam) à des personnes dont l'adresse email est utilisée sans leur accord préalable et avec lesquelles l'expéditeur (le spammeur) n'a jamais eu de contact. Le spam par envoie massif de messages infectés peut contribuer à la propagation rapide de virus (spam + virus), des moteurs de messagerie sont embarqués dans le code des virus afin qu'ils puissent s'auto-diffuser;

– l'usurpation d'identité des utilisateurs (un intrus se fait passer pour quelqu'un d'autre, un élément du système émet, écoute, intercepte des messages qui ne lui sont pas destinés, etc.);
– des messages peuvent être introduits, rejoués, mélangés, supprimés, retardés;
– un refus de service par défection d'un élément de la chaîne du système de messagerie;
– la divulgation d'informations confidentielles;
– la répudiation (un acteur du système nie avoir envoyé ou reçu un message).

Figure III.8 – Architecture SSL (*Secure Socket Layer*)



A ceux-ci on associe également toutes les menaces liées aux réseaux et à leurs modes de fonctionnement (attaques au niveau du routage, des serveurs de noms, etc.).

Pour pallier ces limites sécuritaires inhérentes au mode de fonctionnement de la messagerie, les nouvelles versions de ces logiciels intègrent des facilités de chiffrement pour assurer confidentialité, intégrité et authenticité des informations échangées et des correspondants.

Les impératifs de sécurité des systèmes de messagerie s'expriment en termes:

– de confidentialité et d'intégrité (d'un message ou d'une séquence de messages);
– de non-répudiation (preuve de l'émission, preuve de la réception, signature, certification des messages);
– d'authentification de l'identité de tous les acteurs du système de messagerie (utilisateurs, éléments intermédiaires, mémoire de messages, agents de transfert de messages, etc.).

Le risque le plus important est sans doute celui lié à l'introduction de virus, vers ou cheval de Troie via un message. Une parade à mettre en place consiste à installer un anti-virus sur chaque système afin de déceler la présence d'un virus et si possible de le désinfecter. Un anti-virus ne détecte que les virus pour lesquels il a été conçu et ne protège pas contre de nouvelles formes d'infection et leur nécessaires mise à jour demandent un effort de gestion non négligeable.

Une mesure complémentaire revient à mettre en place un serveur de messagerie de désincubation qui examine systématiquement tous les messages et leurs pièces jointes. Plusieurs anti-virus peuvent alors s'exécuter simultanément et augmenter ainsi la probabilité de détection d'un message infecté.

Le protocole initial de messagerie SMTP (*Simple Mail Transfer Protocol*) de l'environnement internet s'est vu enrichi au cours du temps pour supporter, d'une part, des contenus de message multimédia et d'autre part, pour intégrer des mécanismes de sécurité. Plusieurs sont disponibles actuellement. Parmi eux citons: *Secure Multipurpose Internet Mail Extensions Secure MIME* (S/MIME), *Privacy Enhanced Mail* (PEM) et *Pretty Good Privacy* (PGP).

Toutes les applications du monde internet font appel directement ou non, aux services offerts par un serveur DNS (*Domain Name Server*) (gestion de la relation entre un nom logique et une adresse IP correspondante). Les DNS contribuent activement à la réalisation de l'acheminement correcte des informations. Ainsi, ils constituent des points sensibles de l'architecture de communication et sont donc des serveurs à protéger. La mise en place de mécanismes de sécurité (contrôle d'accès, d'authentification, de trace, de duplication, de cohérence, chiffrement des requêtes et de leurs réponses, etc.) permettront d'éviter que des personnes mal intentionnées ne modifient la valeur des informations qui y sont stockées pour un routage des informations vers des destinataires différents que ceux prévus initialement (détournement), ne les submergent de requêtes inutiles pouvant occasionner des dénis de service à l'indisponibilité des ressources, à l'effondrement du réseau, ne créent de faux serveurs de noms afin d'obtenir des réponses erronées conduisant à des erreurs de transmission ou à des intrusions.

III.2.6 Détection d'intrusion

Intrusions, incidents, anomalies doivent être détectés et identifiés au plus tôt de leur survenue et faire l'objet d'une gestion rigoureuse afin d'assurer le fonctionnement normal des systèmes et leur protection.

Un incident est un évènement qui survient inopinément. Il est le plus souvent sans gravitée en lui-même mais il peut engendrer des conséquences graves. Une anomalie est une exception, elle peut induire un fonctionnement anormal du système d'information pouvant conduire à une violation de la politique de sécurité en vigueur. Elle peut être d'origine accidentelle (par exemple une erreur de configuration) ou volontaire (une attaque ciblée du système d'information). Une intrusion est caractéristique d'une attaque et peut être considérée comme un incident ou une anomalie.

La détection d'intrusion est l'ensemble de pratiques et de mécanismes utilisés afin de détecter des erreurs qui pourraient conduire à des violations de la politique de sécurité et de diagnostiquer les intrusions et les attaques (sont inclus la détection d'anomalies et l'usage abusif des ressources)[46].

Un système de détection d'intrusions (IDS – *Intrusions Detection System*) se compose de trois blocs fonctionnels essentiels: la collecte des informations, l'analyse des informations récupérées, la détection des intrusions et les réponses à donner à la suite d'une intrusion décelée.

III.2.7 Cloisonnement des environnements

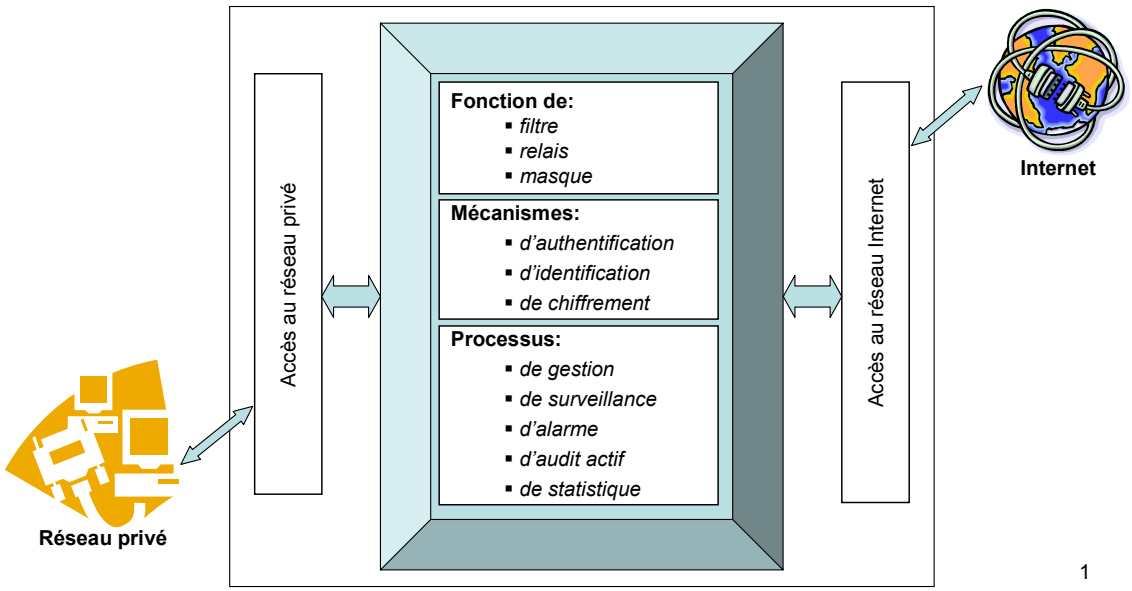
La séparation et le masquage d'un environnement privé vis-à-vis de l'internet public repose sur l'installation d'un ou plusieurs systèmes pare-feu (*firewalls*).

---

46 Alessandri, D. et Al. «Towards a taxonomy of intrusion detection systems and attacks» www.domino.watson.ibm.com/library/cyberdig.nsf/papers/5FA980EB952E09D085256AC600535997/$File/rz3366.pdf

Un *firewall* est un système qui permet de bloquer et de filtrer les flux qui lui parviennent, de les analyser et de les autoriser s'ils remplissent certaines conditions, de les rejeter dans le cas contraire. Le cloisonnement d'un réseau permet de constituer des environnements IP disjoints, en rendant physiquement indépendants les accès des réseaux que l'on désire séparer. Cela permet d'interconnecter deux réseaux de niveaux de sécurité différents (Figure III.9)[47].

Figure III.9 – Structure fonctionnelle d'un *firewall*



Selon la nature de l'analyse et des traitements effectués par un *firewall*, différents types de *firewalls* existent. Ils se distinguent le plus souvent en fonction du niveau de filtrage des données auquel ils opèrent: niveau 3 (IP), niveau 4 (TCP, UDP) ou niveau 7 (FTP, HTTP, etc.) du modèle OSI.

Un *firewall* applicatif encore dénommé proxy (serveur proxy, *firewall proxy*) joue un rôle de relais applicatif. Il établit en lieu et place de l'utilisateur le service invoqué par celui-ci. L'objectif d'un système qualifié de proxy est de réaliser un masquage d'adresse par relais applicatif, et de rendre transparent l'environnement interne de l'organisation. Il est censé constituer un point de passage obligé pour toutes les applications qui nécessitent un accès internet. Cela suppose qu'une application «relais» soit installée sur le poste de travail de l'utilisateur et sur le *firewall*.

L'implantation et la configuration d'un *firewall* résultent d'un choix d'architecture de réseaux pour répondre aux besoins de sécurité et de contrôle demandes de connexion aux systèmes.

Le *firewall* constitue un des outils de réalisation de la politique de sécurité et n'est qu'un des composants matériel ou logiciel de sa mise en œuvre. En effet, un *firewall* ne suffit pas à bien protéger le réseau et les systèmes d'une organisation. Il doit être également accompagné d'outils, de mesures et de procédures répondant à des objectifs de sécurité préalablement déterminés par la politique de sécurité. L'efficacité d'un *firewall* dépend essentiellement de son positionnement par rapport aux systèmes qu'il doit protéger, de sa configuration et de sa gestion.

Si les systèmes *firewall* ou de détection d'intrusion, contribuent à réaliser certains services de sécurité, ils ne suffisent pas à eux seuls à accomplir la protection des ressources informationnelles.

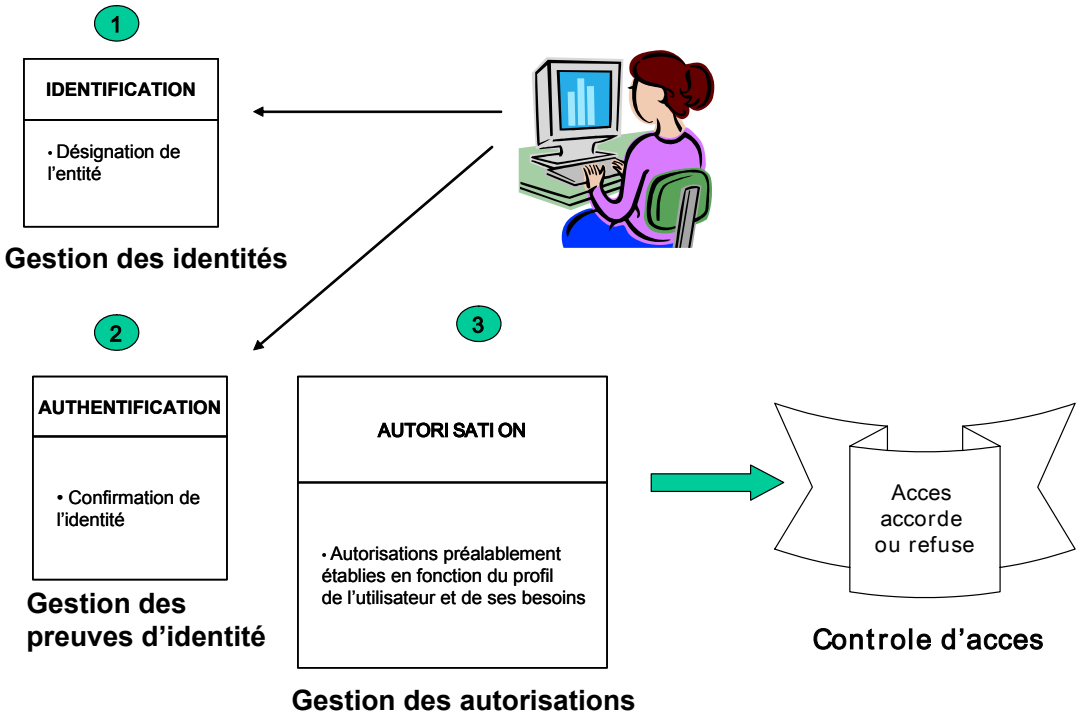
47 Figure issue du livre «Sécurité informatique et télécoms: cours et exercices corrigés»; S. Ghernaouti-Hélie; Dunod 2006.

III.2.8 Contrôle d'accès

III.2.8.1 Principes généraux

Un mécanisme de contrôle d'accès logique aux ressources informatiques est basé sur l'identification des personnes, leur authentification et sur les permissions ou droits d'accès qui leurs sont accordés (Figure III.10).

Figure III.10– Les bases des éléments du contrôle d'accès logique



Sur la base d'une identification authentifiée, le mécanisme de contrôle d'accès accorde, en fonction du profil de l'utilisateur, l'accès aux ressources sollicitées. Cela suppose que l'identification de l'usager (Gestion des identités – *Identity management*), que les preuves de son identité (gestion des preuves de l'identité – *Identity proof management*) et que ses droits d'accès, soient correctement gérés (gestion des autorisations – *Authorization management*).

Le profil de l'usager (*user profile*) regroupe toutes les informations nécessaires aux décisions d'autorisation d'accès. Il doit être défini avec soin et résulte de la définition de la politique de gestion des accès.

L'authentification permet de lier la notion d'identité à une personne. Les autorisations d'accès permettent de filtrer sélectivement les demandes d'accès aux ressources et aux services offerts via le réseau afin d'en accorder l'accès qu'aux seules entités habilitées.

Le service d'authentification a pour objectif de vérifier la véracité de l'identité (notion de preuve de l'identité). Cela dépend généralement d'un ou de plusieurs des facteurs suivants:

– d'un secret qu'une entité détient (ce qu'elle sait), mot de passe ou numéro d'identification personnel (PIN – Personal Identification Number);
– de ce qu'elle possède (carte, jeton, etc.);
– de ce quelle est (empreinte digitale, vocale, rétinienne, etc.).

La vérification de l'identité dépend d'un scénario où le demandeur d'accès donne son identité et une preuve qu'il est censé être le seul à connaître ou à posséder (mot de passe, clé confidentielle, empreinte). Le service d'authentification procède à une comparaison de ces informations avec des données préalablement enregistrées dans un serveur d'authentification.

Un serveur d'authentification doit être hautement protégé et sécurisé par des mécanismes ad'hoc de contrôle d'accès, de gestion sécurisée de systèmes et par le chiffrement des données qu'il stocke. Un serveur d'authentification ne doit pas être défaillant ou vulnérable car de sa robustesse dépend le niveau de sécurité globale de l'infrastructure informatique et télécoms.

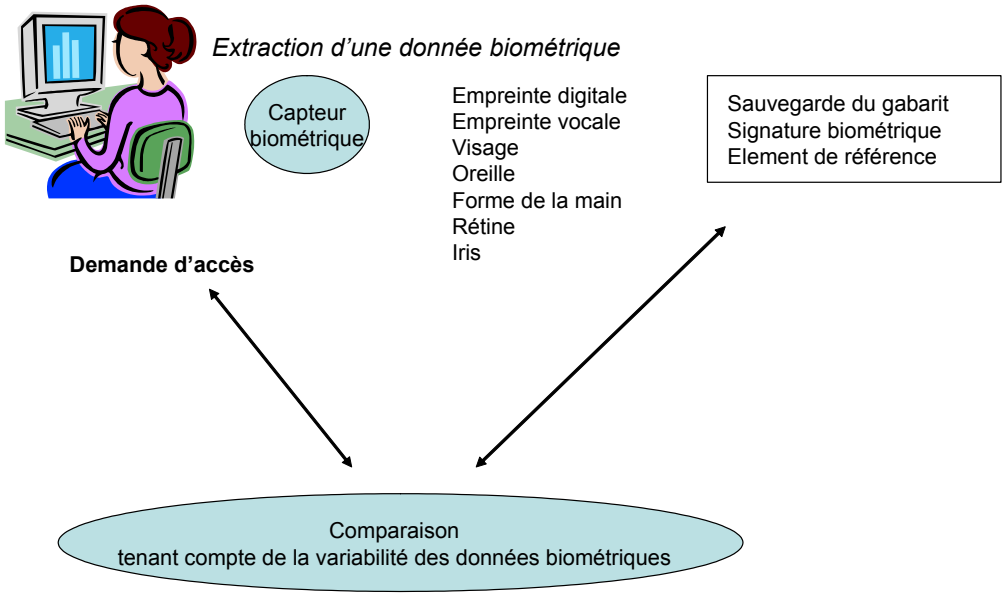
III.2.8.2 Apports et limites de la biométrie

L'individualisation biométrique est une méthode d'individualisation à partir de données biométriques, qui peut servir à contrôler l'identité d'un individu afin de réaliser un contrôle d'accès à des locaux ou dans le cadre d'un contrôle judiciaire (police, etc.).

L'application de la biométrie au contrôle d'accès aux ressources informatiques permettrait de se soustraire de l'usage de mot de passe en les substituant par une caractéristique physique dont on pourrait aisément extraire une donnée binaire.

Afin d'utiliser des caractéristiques physique des personnes pour les identifier et valider leur identification, il est nécessaire d'extraire et d'enregistrer au préalable les caractéristiques biométriques des individus (notion de gabarit). Ces enregistrements doivent être réalisés d'une manière fiable et sauvegardés de façon sécurisée (Figure III.11).

Figure III.11 – Contrôle d'accès biométrique



La durée du processus d'authentification peut être long car la phase de comparaison doit tenir compte des variations inhérentes à la caractéristique vivante de la donnée testée. Un échantillon vocal par exemple n'est jamais strictement le même. La comparaison est basée sur un traitement statistique et probabilistique de la donnée biométrique. Cette part de flou introduit dans le système d'authentification ne permet d'avoir des résultats d'authentification avec un degré d'exactitude certain Le système ne peut pas certifier à 100% qu'il s'agisse de la personne «x». Le taux d'erreur de ces systèmes reste encore élevé, ce qui ne permet pas de garantir un haut niveau de sécurité. Associé à des mécanismes d'authentification «classiques» basé sur des mots de passe, (notion de double contrôle), la biométrie renforce le niveau de sécurité de ces derniers.

De plus, l'usage étendu du biométrique soulève de nombreux problèmes d'éthique et d'ergonomie mais aussi d'ordre économique, juridique et technologique. Pour n'en citer que quelques uns, retenons:

- la confidentialité de données biométriques qui peuvent être considérées comme privées;
- la possibilité de ne pas avoir des données biométriques uniques (cas des vrais jumeaux);
- les capteurs de données biométriques sont souvent perçus comme étant intrusifs, et sont rejetés par la majorité des utilisateurs s'ils en ont la possibilité et le choix! Ils constituent également une menace pour la liberté individuelle dans la mesure ou il pourrait exister une prolifération de capteurs comme des caméras vidéo par exemple, disséminés dans des environnements publics, qui agiraient à l'insu des citoyens;
- les cas d'usurpation ou d'usages abusifs, frauduleux de données biométriques.

Associés à leur manque de précision et aux coûts d'acquisition, de déploiement et de contrôle qui demeurent élevés, les solutions de contrôle d'accès basées sur l'usage de données biométriques ne sont pas communément adoptées.

Récapitulatif des limites de l'usage de données biométriques pour le contrôle d'accès:

1 les données biométriques contribuant à identifier un individu varient au cours du temps;
2 les données biométriques doivent être saisies pour constituer un échantillon de référence qui sera sauvegardé dans une base de données. En devenant numériques ses données deviennent fragiles (et donc modifiables), elles devront être protégées de manière optimale. A chaque demande d'accès, les données biométriques de l'utilisateur devront être captées. Ceci pose un problème d'acceptation de la méthode de saisie, le sentiment d'intrusion est souvent mal toléré;
3 la technique de contrôle d'accès basée sur l'usage du biométrique n'est pas sûre à 100%, du fait de la variabilité de l'échantillon humain dont le processus d'authentification doit tenir compte. Selon les systèmes, la probabilité d'avoir des faux positifs ou des faux négatifs peu être importante. Cette probabilité dépend de la technique et de la qualité d'enregistrement des données biométriques.

III.2.9 Protection et gestion des infrastructures de communication

III.2.9.1 Protection

La couche 1 ou physique peut, contribuer à la sécurité des transmissions en effectuant du brouillage de ligne, c'est-à-dire, en envoyant de l'information non significative pour masquer un flux de données pertinentes dans un flux ininterrompu de données sans importance. Toutefois, s'il fallait protéger les transmissions contre des écoutes passives réalisées par capture des rayonnements électromagnétiques induits par le signal véhiculé sur les supports de transmission, il faudrait isoler complètement ces derniers dans des cages de Faraday. On comprend qu'une telle mesure de protection ne sera réalisée qu'en cas de nécessité.

La sécurité physique des supports de transmission, des boîtiers de raccordement et des équipements de connectique doit être assurée correctement.

L'infrastructure de transmission est à protéger contre d'éventuels rayonnements qui pourraient compromettre la transmission des données et contre des attaques passives (écoute des données) ou actives (modification, destruction, création de données).

Il est impératif de savoir protéger les raccordements des utilisateurs. Pour cela, il faut les identifier «qui sont les usagers?», les localiser «où sont-ils?» et connaître leurs besoins «quels sont les flux applicatifs transportés?». En répondant à la question générale consistant à savoir «qui fait quoi et où?» on distingue les différents besoins sécuritaires du réseau de transport.

Sécuriser le transfert de données, revient à intégrer les processus de sécurité au niveau de l'infrastructure de communication qui doit donc être à même de la supporter dans son intégralité. Cela nécessite le plus souvent la mise à jour de l'ensemble des routeurs, pouvant parfois conduire à des problèmes d'interopérabilité de ceux-ci et de gestion du changement.

De plus, chiffrer les données au niveau «réseau» génère des paquets de données de taille supérieure à des paquets non chiffrés; leur transfert monopolise donc plus de bande passante et de ressources de communication. Associées au fait que le processus de chiffrement augmente le temps de traitement des paquets, les performances du réseau peuvent considérablement être affectées par la mise en œuvre de la sécurité à ce niveau.

L'avantage principal du chiffrement au niveau de l'infrastructure du réseau, réside dans l'indépendance de l'application et des mécanismes de chiffrement liés au transfert qui sont alors complètement transparents pour l'utilisateur.

En revanche, la sécurité des transactions au niveau applicatif (chiffrement des données au plus près de l'application qui les manipule) modifie l'application elle-même et les données sont chiffrées avant d'être livrées au protocole de réseau qui en effectuera leur acheminement. Elles sont ensuite déchiffrées par le serveur d'application destinataire. C'est lors de la phase d'établissement du dialogue entre des entités applicatives (un client et un serveur par exemple) que l'on réalise l'authentification et la négociation d'une clé de session. La complexité de cette phase peut varier et demande un délai d'établissement lui aussi variable. Une fois réalisé, le chiffrement est en général assez rapide. Il est indépendant de la plate-forme d'exécution et de l'infrastructure de communication.

La protection au niveau de la sphère de travail de l'utilisateur qui met en œuvre une application distribuée, ne dépend plus du transporteur de données, ni du réseau, mais bien de l'environnement direct de l'usager. La difficulté de la protection des applications réside dans le fait qu'il faille protéger tout l'environnement applicatif, le poste de travail de l'utilisateur (et non plus seulement l'application elle-même) et par extension son environnement physique (accès aux locaux, etc.).

Protéger les applications revient à garantir le droit des individus par rapport aux postes de travail, aux applicatifs, à la zone géographique dans laquelle elles s'intègrent.

Les fonctions de base du système d'exploitation du poste de travail de l'utilisateur jouent un rôle prépondérant dans cette protection (impossibilité de prendre la main lors d'une session, déconnexion automatique après un certain temps, etc.). Cela passe également par la protection des cartes réseaux, par le support de protocoles d'application en mode sécurisé (transmission de fichiers protégés, messagerie sécurisée, etc.), par des opérations de *mirroring* et de *duplexing* (protection des informations en les dupliquant sur des disques, redondance des opérations d'écriture et des équipements).

Sécuriser l'infrastructure de transport ou sécuriser l'application revient à traiter, à des niveaux différents, un même problème:

- les processus et les utilisateurs doivent être authentifiés;
- l'émetteur et le récepteur utilisent un algorithme de chiffrement/déchiffrement identique;
- chaque entité communicante doit avoir connaissance de l'algorithme et des clés de chiffrement/déchiffrement;
- les clés de chiffrement/déchiffrement doivent être gérées;
- les données doivent être formatées pour être transférées.

III.2.9.2 Gestion

Les activités de gestion de systèmes et de réseaux lorsqu'elles sont menées correctement, permettent d'offrir les niveaux de disponibilité et de performance nécessaires à la réalisation de la sécurité. De plus, elles intègrent les tâches de surveillance du réseau, de détection des anomalies ou incidents (comme les intrusions par exemple), qui contribuent grandement à la sécurité globale du réseau et du système d'information qu'il dessert.

Une bonne gestion de réseaux contribue à rendre les infrastructures, services et données disponibles et de cela de manière performante. Par la gestion de réseau, notamment par les fonctions de gestion des configurations, des performances et des incidents, les objectifs de sécurité que sont la disponibilité et l'intégrité, peuvent être atteints.

De plus, la dimension de gestion de réseaux qui fait référence à la gestion comptable permet de disposer de toutes les données nécessaires non seulement à la facturation des usagers mais aussi à la réalisation des fonctions de surveillance et d'audit qui sont de première importance en matière de sécurité. Cela peut permettre une certaine vérification des actions à des fins de preuve ou de non-répudiation.

La gestion de réseau contribue également à réaliser l'objectif de confidentialité dans la mesure elle assure qu'il n'y ait pas d'écoutes clandestines ou des accès non autorisés aux données. La réalisation de la fonction de contrôle d'accès aux ressources qui fait partie de la gestion de réseau, est fondamentale à la mise en œuvre opérationnelle de la sécurité.

C'est de la qualité de gestion des routeurs, des facilités d'adaptation de leur décision de routage en fonction de l'état du réseau et des demandes d'acheminement du trafic, que dépendent en grande partie les performances, la qualité de service, la disponibilité et la fiabilité d'un réseau. La mise à jour des tables de routage des grands réseaux est un vrai casse-tête opérationnel pour les administrateurs de réseaux, dans la mesure où les différentes modifications des valeurs des tables doivent être synchronisées pour éviter les dysfonctionnements et les pertes de données en transit. Les protocoles de gestion de réseau permettent, entre autres, de mettre à jour les tables de routage. L'administration de réseau peut contribuer à la sécurisation des routeurs en y effectuant des accès sécurisés lors de leur configuration, en générant des alarmes lors de tentative d'intrusion, et en sécurisant les centres de gestion et de supervision des routeurs.

Il est donc crucial de savoir la protéger en empêchant tout un chacun de l'altérer en prévenant ou détectant, entre autres, les actions suivantes:

- modification des adresses contenues dans les tables de routage, dans les paquets IP, etc.;
- modification des routes, copies illicites des données transportées;
- surveillance des flux;
- détournement, modification et destruction de paquets de données;
- déni de service, effondrement des routeurs, inondation du réseau, etc.

Il est important de pouvoir sécuriser les processus d'acheminement des données au travers des réseaux de télécommunication. Les fournisseurs de service «réseau» doivent protéger toutes les entités qui interviennent dans ce processus notamment les routeurs et les serveurs de noms afin que la qualité du service d'acheminement satisfasse les critères de sécurité de disponibilité (le service est opérationnel), de confidentialité (les données sont délivrées aux bons destinataires) et d'intégrité (les données ne sont pas modifiées lors de leur transfert).

La livraison de données aux ayants droits n'est pas garantie par un service réseau. En effet, le service de livraison correcte ne vérifie pas que les données délivrées à la bonne adresse le sont aux entités habilitées à les recevoir. Cela nécessite un contrôle supplémentaire de type «contrôle d'accès». De plus, si les données sont véhiculées en clair et si elles sont écoutées, elles sont compréhensibles à des tiers non autorisés. S'il s'agit de données sensibles il est nécessaire de les chiffrer pour les rendre inintelligibles.

La surveillance d'un réseau informatique consiste à observer le fonctionnement de ce dernier et ceci d'une manière continue. La surveillance du réseau vise non seulement à s'assurer que la qualité de service du réseau soit acceptable mais aussi à déceler les problèmes, incidents, erreurs et les anomalies qui dégradent les performances du réseau et qui pourraient porter atteinte à la sécurité des ressources afin de répondre au plus vite et de manière adaptée aux disfonctionnements. La fonction de surveillance du réseau permet la traçabilité des actions et des évènements afin de les journaliser pour les analyser (notion d'audit). La surveillance du réseau, contribue également à s'assurer de la disponibilité des ressources en vérifiant que le réseau fonctionne d'une manière correcte. Ainsi, il s'agit d'une fonction cruciale de la gestion de réseau puisqu'elle contribue à réaliser la gestion des performances, des incidents, des configurations, des utilisateurs et de la sécurité

SECTION IV

APPROCHE GLOBALE

Chapitre IV.1 – Différents aspects du droit des nouvelles technologies

IV.1.1 Protection des données à caractère personnel et commerce électronique[48]

Ce paragraphe aborde la protection des données personnelles concernant notamment le cybercommerce et identifie, à partir de la situation en France et en Suisse, les principales législations dont les administrateurs systèmes et responsables sécurité doivent avoir connaissance lors que leur organisations met en ligne des services de commerce électronique. Ainsi, peuvent être extrapolés et adaptés aux pays en développement, les principes généraux qui pourraient adoptés pour conduire des affaires dans le cyberespace.

IV.1.1.1 Cybercommerce: ce qui est illégal «off-line» l'est aussi «on-line»

Lorsque l'on aborde la question du commerce électronique (e-commerce), on peut envisager la problématique sous les angles du commerce électronique avec les consommateurs (*business-to-consumer* (B2C)), ou du commerce électronique inter-entreprise (*business-to-business* (B2B)). On classera également dans la même catégorie les variantes associées par exemple à la cyberadministration. Il s'agit alors de commerce électronique avec le citoyen et d'autres institutions publiques ou privées. Cette distinction est importante au niveau juridique puisque le droit commercial différencie en général les transactions inter-entreprises de celles opérées avec le consommateur.

Dans tous les cas, la sécurité, conjuguée à des démarches appropriées de marketing et de vente sur l'internet, respectant un cadre légal approprié, constitue la pierre angulaire du cybercommerce. Réaliser un contexte favorable à l'échange de données par le biais de l'instauration de la confiance basé sur les outils de la sécurité et le respect des législations, favorise l'adoption par le grand public de services basés sur l'informatique et les télécommunications et permet également de développer une véritable économie de services.

De nouvelles législations, nées de la nécessité de définir un cadre juridique approprié à l'usage des nouvelles technologies, viennent compléter la plus part des législations existantes qui sont également valides dans le cyberespace. En tout état de cause, ce qui est illégal «off-line» l'est aussi «on-line»! Le cyber espace est un espace international et transfrontalier. De ce fait, la notion du for est très difficile à cerner pour pouvoir régler les problèmes juridiques du commerce électronique. Ainsi, lors de transactions effectuées par le biais du Net il est nécessaire de mentionner la limite de l'offre et de donner une information exacte quant au for à considérer en cas de litige.

IV.1.1.2 Devoir de protection

La protection des données personnelles est un aspect important du commerce électronique. Le consommateur doit être informé de la nature des informations collectées, utilisées et communiqués par l'annonceur ou le commerçant en ligne. Le consommateur doit être informé à l'avance quant à l'utilisation, la communication, l'accès par les tiers à des informations le concernant. Il doit être également informé des précautions prises pour protéger les informations le concernant. Une réelle politique de protection des données privées (*privacy policy*) doit être clairement exprimée, disponible, visible, facilement accessible et compréhensible au moment où est entreprise transaction commerciale. La politique doit être notamment disponible sur le site web du commerçant.

De plus, cela nécessite de la part de l'entreprise fournisseur de service de mettre en œuvre les moyens de sécurité suffisants pour protéger les données des clients collectées et traitées. L'entreprise doit prendre soin de s'assurer que les services tiers impliqués dans les échanges commerciaux disposent des niveaux de sécurité apte à satisfaire les impératifs de sécurité.

---

48 Ce point à été élaboré en collaboration avec Igli Taschi, assistant diplômé de l'Université de Lausanne.

IV.1.1.3 Respect des droits fondamentaux

La confidentialité des données à caractère personnel et celui du respect de l'intimité numérique relèvent du respect des droits fondamentaux de l'Homme.

Exemple de la directive européenne

Outre la directive européenne de 1995, remarquons que diverses législations nationales existent depuis le début des années 70 concernant la protection des données personnelles et le contrôle de l'utilisation des fichiers publics contenant des informations nominatives afin de prévenir des risques de fichage inconsidéré.

Exemple de la France

La Loi «Informatique et liberté» publiée en janvier 1978 est un exemple de ce type d'initiative juridique pour la France qui a été modifiée par la nouvelle Loi informatique et liberté publiée en août 2004 et immédiatement applicable. Celle-ci introduit des concepts juridiques adaptés aux nouvelles formes de traitements issus de la société de l'information et de l'économie numérique. Elle transpose la directive communautaire 95/46/CE d'octobre 1995. Son objet est de renforcer les droits et protections reconnus aux personnes physiques et d'augmenter le niveau d'obligations incombant aux responsables de traitements.

Sont généralement abordés dans ces lois les questions relatives à la définition d'une information nominative ou à caractère personnel; au droit d'accès, d'opposition et de rectification aux données; la finalité du traitement; la collecte d'information;la conservation et la mise à jour; la sécurité des fichiers nominatifs; la commercialisation des fichiers: le contrôle des flux transfrontaliers.

D'autres lois viennent le plus souvent compléter ces législations comme par exemple pour la France la loi sur la sécurité quotidienne du 15.11. 2001 qui oblige à effacer et à rendre anonyme les données relatives à une communication électronique sauf celles concernant la facturation des communications. Les données dites «indirectes» (URL visités, les adresses IP des serveurs consultés, les intitulés des messages, etc.) doivent être également effacés.

Exemple de la Suisse

En Suisse la loi fédérale sur la protection des données date de 1992 (Allemagne: loi du 21 janvier 1977, Belgique: loi du 8 décembre 1992, Canada: loi sur la protection des renseignements personnels –1982S, Etats-Unis: loi sur la protection des libertés individuelles –1974; loi sur les bases de données et la vie privée –1988)

La protection des données en Suisse est en premier lieu assurée par l'art. 13 al. 2 de la nouvelle Constitution fédérale, entrée en vigueur le 1er janvier 2000, en vertu duquel «*toute personne a le droit d'être protégée contre l'emploi abusif des données qui la concernent*».

Les textes les plus importants sur le plan fédéral sont la *loi fédérale sur la protection des données* (LPD) du 19 juin 1992 et l'ordonnance d'exécution du 14 juin 1993. Son application ne dépend pas d'un support particulier ou d'une technique spécifique de récolte et de traitement des données. Elle s'applique aussi bien aux personnes privées qu'à l'administration publique, aux personnes physiques et aux personnes morales, quel que soit le type de traitement visé. L'article 3, lettre a) de la LPD précise qu'il faut entendre par données personnelles «*toutes les informations qui se rapportent à une personne identifiée ou identifiable*». Des règles particulières s'appliquent aux données sensibles et aux profils de la personnalité, notions également définies par la loi.

La notion de traitement est large puisqu'elle inclut «*toute opération relative à des données personnelles – quels que soient les moyens et procédés utilisés – notamment la collecte, la conservation, l'exploitation, la modification, la communication, l'archivage ou la destruction de données*». L'art. 2 al. 2 LPD réserve pourtant un certain nombre de situations particulières dans lesquelles la loi n'est pas applicable. C'est par exemple le cas pour des procédures judiciaires pendantes ou dans l'hypothèse de «*données personnelles qu'une personne physique traite pour un usage exclusivement personnel et qu'elle ne communique pas à des tiers*» (litt. a). Dans un arrêt du 5 avril 2000, le Tribunal fédéral a considéré que la messagerie électronique était couverte par le secret

des télécommunications. L'art. 43 de la Loi fédérale sur les télécommunications (LTC) contient également une obligation de maintien du secret: «Il est interdit à toute personne qui a été ou qui est chargée d'assurer un service de télécommunication de donner à des tiers des renseignements sur les communications des usagers; de même, il lui est interdit de donner à quiconque la possibilité de communiquer de tels renseignements à des tiers». L'article 44 LTC, complété par les articles 6 à 11 de l'Ordonnance du Conseil fédéral sur le service de surveillance de la correspondance postale et des télécommunications du 1er décembre 1997 (RS 780.11), met en place la procédure et détaille les conditions auxquelles une surveillance peut intervenir.

La réglementation suisse sur la protection des données personnelles sur l'internet est similaire à bien des égards à celle de la Directive communautaire en la matière.

IV.1.1.4 Rentabilité de la législation

La législation en matière de traitement des données à caractère personnel et de protection de la vie privée dans le secteur des communications électroniques, est un facteur qui pousse les institutions à bien gérer leur sécurité informatique et réseau (données des utilisateurs, surveillance des communications et des employés, gestion des sauvegardes, traitement automatisé de données à caractère personnel, etc.).

Les organisations se doivent de se doter de moyens suffisants de sécurité et de contrôle.

La valeur économique des investissements nécessaires à assurer le seuil minimal de sécurité (protection physique et juridique) est fonction des pertes matérielles et aussi des risques de réputation et d'image potentiellement encourus par l'organisation. La législation devient donc un facteur endogène de prise en compte de la sécurité.

IV.1.2 Cybercommerce et réalisation de contrats dans le cyberespace[49]

Ce paragraphe aborde différents aspects de la notion de contrat associée aux transactions commerciales réalisées dans le cyberespace et identifie les principaux textes de lois existants en Suisse et au niveau européen, qui les régissent. A partir de l'exemple juridique de la Suisse, et des principales directives européennes, divers principes de base peuvent être identifiés et adaptés en fonction des pays et des législations nationales.

IV.1.2.1 Question du droit applicable

La première problématique juridique qui concerne le commerce électronique est posée par la définition de la notion géographique de la réalisation du commerce électronique. Les caractéristiques de l'internet (couverture internationale, technologies du numérique, mode de fonctionnement) abolissent la notion de frontières géographiques des états et les flux informationnels ne s'arrêtent pas aux frontières des pays.

Données et services sont accessibles et réalisables à distance, indépendamment de la localisation des internautes et des serveurs. Très souvent le commerçant et le client interagissent depuis des pays différents. Ainsi la notion du droit applicable devient très importante en cas de litige éventuel et constitue un point capital concernant la planification de l'offre. Dans ce sens lors des transactions fait par le biais du Net il faut mentionner la limite de l'offre et donner une information exacte quant au for[50] à considérer en cas de litige.

Le droit applicable et le for peuvent être convenus par les parties au contrat. Si une telle clause n'existe pas, il faut déterminer si le contrat tombe dans le champ d'application d'une convention internationale telle que celle des Principes Unidroit relatifs au contrat du commerce international (1994) *autrement dit la Netiquette* ou bien la Convention de la Haye du 15 juin 1955 par exemple.

---

[49] Ce point à été élaboré en collaboration avec Igli Taschi, assistant diplômé de l'Université de Lausanne.

[50] For: En droit international, désigne la loi du pays dans lequel le procès doit se dérouler. On parle également de lex fori. *Règle de procédure internationale*

Toutefois, les conventions internationales n'ont pas une force contraignante sauf dans le cas où elles sont expressément intégrées dans le contrat.

Si aucune de ces deux solutions n'est envisageable, se sont les règles de droit régissant le contrat qui seront celles applicables.

En droit suisse par exemple, il s'agit de la loi fédérale sur le droit international privé de 1987 (LDIP), dont l'article 1 stipule:

«Art. 1»

[1] La présente loi régit, en matière internationale:

a. la compétence des autorités judiciaires ou administratives suisses;

b. le droit applicable;

c. les conditions de la reconnaissance et de l'exécution des décisions étrangères;

d. la faillite et le concordat;

e. l'arbitrage.

[2] Les traités internationaux sont réservés.»

Le principe de base est le suivant: on applique le droit de l'Etat avec lequel le contrat présente les *liens les plus étroits* (117/1 LDIP). Généralement, il s'agit du fournisseur des biens et services pour autant qu'il inclut cela d'une manière explicite dans les conditions générales avec une exception, l'article 120/2 LDIP qui concerne les *Contrats conclus avec des consommateurs* et qui stipule que:

«Les contrats portant sur une prestation de consommation courante destinée à un usage personnel ou familial du consommateur et qui n'est pas en rapport avec l'activité professionnelle ou commerciale du consommateur sont régis par le droit de l'Etat de la résidence habituelle du consommateur:

a. si le fournisseur a reçu la commande dans cet Etat;

b. si la conclusion du contrat a été précédée dans cet Etat d'une offre ou d'une publicité et que le consommateur y a accompli les actes nécessaires à la conclusion du contrat, ou

c. si le consommateur a été incité par son fournisseur à se rendre dans un Etat étranger aux fins d'y passer la commande.

[2] L'élection de droit est exclue.»

Le contenu du site comme par exemple le langage utilisé ou les devises proposées peuvent donner une indication sur le marché visé par le commerçant et éventuellement sur le droit applicable.

Concernant le for, dans le cas ou il n'est pas déterminé par un accord des parties, le dépôt d'une plainte au lieu de résidence ou le siége du défendeur est possible.

IV.1.2.2 Conclusion électronique d'un contrat

Les règles applicables en la matière, sont en général les mêmes que celles applicables pour les contrats dits classiques. Un contrat est conclu lorsque les deux parties ont échangé une offre et une acceptation d'offre.

Directive Européenne

La directive 97/7/CE du Parlement européen et du Conseil de l'Europe du 20 mai 1997 traite de la problématique de la vente à distance et de celle du e-commerce, précise que l'information préalable à la conclusion d'un contrat doit comprendre les éléments suivants:

- identité du fournisseur et, dans le cas de contrat nécessitant un paiement anticipé, son adresse;
- caractéristiques essentielles du bien ou du service;
- prix du bien ou du service, toutes taxes comprises;
- frais de livraison, le cas échéant;
- modalités de paiement, de livraison ou d'exécution;

- existence d'un droit de rétractation, sauf dans les cas visés à l'article 6, paragraphe 3 de cette directive;
- coût de l'utilisation de la technique de communication à distance, lorsqu'il est calculé sur une base autre que le tarif de base;
- durée de validité de l'offre ou du prix;
- durée minimale du contrat dans le cas de contrats portant sur la fourniture durable ou périodique d'un bien ou d'un service.

Le point le plus important concernant la conclusion de contrat concerne la définition de ce qui représente l'offre et de ce qui représente l'acceptation de l'offre. La marchandise «exposée» sur un site internet avec les indications de prix, les informations d'ordre publicitaire associées, ne constituent pas une offre, mais plutôt un appel d'offre au sens du Code des Obligations suisse, qui stipule dans son article 7: «*Art. 7 … [2] L'envoi de tarifs, de prix courants, etc., ne constitue pas une offre de contracter…*».

L'envoi d'un message électronique ou d'un formulaire de commande est également considéré comme un appel d'offre.

C'est l'acceptation ou le clic «j'achète» de la part de l'acheteur qui permet de constituer l'offre ferme et le contrat. La simple consultation d'un site ne peut pas exprimer la volonté de consommer comme l'est d'ailleurs de pénétrer dans un magasin. En revanche, la présentation des marchandises sur un site web peut constituer une offre seulement dans le cas ou le stock de marchandise est indiqué de la part de l'offreur et suite à une commande il diminue, ou bien dans le cas ou la nature de la marchandise est telle que le marchand a toujours la capacité de honorer la commande.

Le contrat est conclu quand le destinataire du service, donc le consommateur désirant acheter la marchandise exposée, a reçu par voie électronique de la part du prestataire, l'accusé de réception de l'acceptation uniquement si ces deux documents sont envoyés dans les meilleurs délais. Concernant la notion de délais il faut faire la distinction entre un contrat entre absents ou entre présents.

Contrat conclu entre absents, oui mais…

Le contrat conclu via l'internet est considéré comme étant un contrat conclu entre absents, ce qui implique que l'offre doit être acceptée dans des délais raisonnables, comme le précise l'article 5 du Code des Obligations suisse:

« Art. 5»:

b. Entre absents

[1] Lorsque l'offre a été faite sans fixation de délai à une personne non présente, l'auteur de l'offre reste lié jusqu'au moment où il peut s'attendre à l'arrivée d'une réponse expédiée à temps et régulièrement.

[2] Il a le droit d'admettre que l'offre a été reçue à temps.

[3] Si l'acceptation expédiée à temps parvient tardivement à l'auteur de l'offre, et que celui-ci entende ne pas être lié, il doit en informer immédiatement l'acceptant.»

Toutefois, si l'échange de données concernant le contrat s'effectue via un forum de discussion, *chat*, messagerie instantanée ou par de la téléphonie sur internet, cela sera considéré comme étant un contrat conclu entre les présents et l'acceptation doit être immédiate. Ainsi l'article 4/1 du Code des Obligations suisse fixe: *«Lorsque l'offre a été faite à une personne présente, sans fixation d'un délai pour l'accepter, l'auteur de l'offre est délié si l'acceptation n'a pas lieu immédiatement.»*

IV.1.2.3 Signature électronique

La mise en œuvre d'un système de chiffrement asymétrique permet de vérifier l'intégrité d'un message afin de s'assurer que le message n'ait pas été modifié lors de son transfert et d'être sûre de son émetteur, ainsi, l'émetteur ne pourra pas nier avoir envoyé ce message (notion de non-répudiation). On utilise pour réaliser ces services de sécurité informatique, un certificat numérique qui permet de «signer» un document numérique. Par analogie à la signature manuscrite, on réalise ainsi une signature numérique des données (notion de signature électronique). Sont associés aux

notions de signature et de certificat numériques, celles de clés de chiffrement (clés privées, clés publiques) et d'organisme de certification (également dénommé tiers de confiance ou autorité de certification).

Pour que la signature électronique puisse être considérée comme une transposition dans le monde numérique de la signature manuscrite d'un document papier, la signature électronique doit être liée uniquement au signataire, permettre de l'identifier et doit être créée par des moyens à la possession exclusive du signataire.

En droit suisse, la signature électronique est reconnue par la loi comme ayant la même portée que la signature manuscrite. L'article 14/2bis du Code des Obligations définit la signature: «*Art. 14: …c. Signature*

[1] La signature doit être écrite à la main par celui qui s'oblige.

…

[2bis] La signature électronique qualifiée, basée sur un certificat qualifié émanant d'un fournisseur de services de certification reconnu au sens de la loi du 19 décembre 2003 sur la signature électronique est assimilée à la signature manuscrite. Les dispositions légales ou conventionnelles contraires sont réservées.

…»

Tandis que la signature électronique est régie par la Loi fédérale sur les services de certification dans le domaine de la signature électronique (SCSE) du 19 décembre 2003. C'est dans cette loi qu'est définie la signature électronique ainsi que ses différentes formes et les divers acteurs de la mise en œuvre du mécanisme de signature et de certificats numériques.

«Art. 2 Définitions

Au sens de la présente loi, on entend par:

a. signature électronique: données électroniques jointes ou liées logiquement à d'autres données électroniques et qui servent à vérifier leur authenticité;

b. signature électronique avancée: signature électronique qui satisfait aux exigences suivantes:

1. être liée uniquement au titulaire,

2. permettre d'identifier le titulaire,

3. être crée par des moyens que le titulaire peut garder sous son contrôle exclusif,

4. être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable;

c. signature électronique qualifiée: signature électronique avancée fondée sur un dispositif sécurisé de création de signature au sens de l'art. 6, al. 1 et 2, et sur un certificat qualifié valable au moment de sa création;

d. clé de signature: données uniques telles que des codes ou des clés cryptographiques privées que le titulaire utilise pour composer une signature électronique;

e. clé de vérification de signature: données telles que des codes ou des clés cryptographiques publiques utilisées pour vérifier une signature électronique;

f. certificat qualifié: certificat numérique qui remplit les conditions de l'art. 7;

g. fournisseur de services de certification (fournisseur): organisme qui certifie des données dans un environnement électronique et qui délivre à cette fin des certificats numériques;

h. organisme de reconnaissance: organisme qui, selon les règles de l'accréditation, est habilité à reconnaître et à surveiller les fournisseurs…»

Signature électronique et directive européenne

La Directive CE 1999/93 du 13 décembre 1999 relative à un cadre communautaire pour la signature électronique distingue trois types de signature électronique selon le degré d'intégration des mécanismes de chiffrement et les niveaux de sécurité offerts.

Plusieurs variantes existent pour réaliser une signature électronique. Premièrement, il est juste possible de «signer» un message sans que la signature dépende du contenu du message (notion de signature électronique à proprement parlé). Ainsi n'importe qui peut «détacher» la signature d'un message et la réutiliser en lieu et place du propriétaire de la signature. Pour pallier cet inconvénient, il est possible, par la mise en œuvre d'une fonction cryptographique, de rendre la signature dépendante du contenu à signer et de pouvoir valider à sa réception, l'authenticité de l'émetteur et l'intégrité du message (notion de signature électronique avancée).

Enfin la directive envisage la signature électronique certaine qui doit être basée sur les dispositifs de sécurité de l'annexe II concernant les prestataires de service de certification délivrant des certificats qualifiés[51].

IV.1.2.4 Droit de révocation

La facilité avec laquelle il est possible d'effectuer des achats sur l'internet peut favoriser des comportements de consommation relevant d'une décision irréfléchie. Dans ce contexte, le droit de révocation prend une grande importance.

En suisse, l'article 9 du Code des Obligations régit le droit de révocation. Son principe est le suivant: «le retrait de l'offre sera valable, pour autant qu'il parvienne au destinataire de l'offre avant celle-ci». Le même mécanisme est utilisé pour le retrait de l'acceptation.

Droit de révocation et directive européenne

Au niveau européen c'est la directive 1997/7 du 20 mai 1997 qui régit le droit de révocation. Il est stipulé que pour tout contrat à distance, le consommateur dispose d'un délai d'au moins sept jours ouvrables pour se rétracter sans pénalités et sans indication du motif. Au cas où le fournisseur n'a pas rempli les obligations visées à l'article 5, notamment les modalités du droit de rétraction, le délai est de trois mois.

IV.1.2.5 Gestion des litiges

Dès lors qu'un contrat est valablement conclu, la question de la preuve se pose lors de litige, qu'il s'agisse de l'internet ou non: il est nécessaire d'apporter des preuves. Ainsi, il est toujours judicieux de garder des traces de la transaction comme par exemple une copie d'un message électronique ou encre une copie d'écran.

Exemple de la France

En France l'article 109 du Code de consommation considère la preuve comme étant libre concernant le B2B. Le message électronique est donc admis comme moyen de preuve, de la même façon qu'un document papier. En revanche, pour tout ce qui se rapporte au commerce avec le consommateur, une preuve écrite est exigée à partir d'une certaine somme engagée. Cela dans le but de protéger le consommateur moyen qui n'a pas la capacité et les moyens juridiques de se défendre dans le cas d'un litige face à une entreprise commerciale.

Toutefois, l'utilisation des messages électroniques pourrait également être possible comme moyen de preuve à l'instar de la loi sur la signature électronique. Cela signifie qu'un message électronique signé électroniquement sera considéré comme une preuve valable si les dispositions décrites ci-dessus concernant la signature électronique sont respectés.

---

51 www.foruminternet.org/documents/textes_europeens/lire.phtml?id=34

Conditions générales

Très souvent les contrats conclus à distance comportent des conditions générales qui font aussi partie du contrat. Ces conditions générales doivent être facilement accessibles, consultables en ligne et le client doit être clairement informé qu'elles font partie du contrat, pour les valoir en cas de litige.

On-line Dispute Resolution

Lors de litige et compte tenu du caractère international du e-commerce, d'autres moyens que les tribunaux classiques sont à disposition des intéressés pour résoudre les différends. Le concept d'ODR (*On-line Dispute Resolution*) est issu de cette volonté de trouver des solutions immédiates à des conflits liés au non respect de contrats passés via l'internet. Ce type de résolution des litiges se base sur la conciliation qui fait appel à la négociation, à la médiation et à l'arbitrage[52]. Plus rapide, plus accessible financièrement et convivial pour les utilisateurs. En revanche, du fait que cela se base sur des codes de conduite ou des recommandations qualifiées de «*soft law*» (comme par exemple *Uniform Domain-Name Dispute Resolution Policy* de l'ICANN), leur force contraignante est limitée.

IV.1.3 Cyberespace et propriété intellectuelle[53]

IV.1.3.1 Protection de la propriété intellectuelle par des lois

La propriété intellectuelle est protégée par plusieurs lois dont essentiellement:

- loi sur les marques;
- loi sur le droit d'auteur;
- loi sur les brevets;
- loi sur les dessins et modèles;
- loi sur la protection des obtentions végétales;
- loi sur les topographies de semi-conducteurs;
- loi sur les armoiries publiques et autres signes publics.

De plus, la propriété intellectuelle est aussi concernée par la loi contre la concurrence déloyale.

IV.1.3.2 Droit d'auteur et droits voisins

Il s'agit d'une loi qui protège les:

- auteurs d'œuvres littéraires et artistiques;
- artistes interprètes, producteurs de phonogrammes ou de vidéogrammes ainsi que des organismes de diffusion.

Une œuvre est une création de l'esprit, littéraire ou artistique, qui a un caractère individuel et ce indépendamment de sa valeur ou sa destination.

Les créations de l'esprit incluent:

- les œuvres recourant à la langue qu'elles soient littéraires, scientifiques, ou autres;
- les œuvres musicales et autres œuvres acoustiques;
- les œuvres des beaux-arts, en particulier, les sculptures et les œuvres graphiques;
- les œuvres à contenu scientifique ou technique, tels que les dessins, les plans, les cartes ou les ouvrages sculptés ou modelés;
- les œuvres d'architecture;
- les œuvres des arts appliqués;

---

[52] Ce mécanisme de résolution de conflit a fait l'objet d'un règlement type de la Commission des Nations Unies pour le droit commercial international (CNUDCI).

[53] Ce point a été élaboré en collaboration avec le professeur Sarra Ben Laggha, Ecole Polytechnique de Tunis, chargé de cours à l'Université de Lausanne.

- les œuvres photographiques, cinématographiques et les autres œuvres visuelles ou audiovisuelles;
- les œuvres chorégraphiques et les pantomimes;
- les programmes d'ordinateurs (logiciels);
- les projets, titres et parties d'œuvres qui ont un caractère individuel.

Le droit d'auteur accorde à l'auteur de l'œuvre (la personne physique qui a créé l'œuvre) ou son auteur présumé (la personne qui a fait apparaître l'œuvre tant que l'auteur n'est pas désigné) des droits moraux et des droits patrimoniaux.

Le dépôt de l'œuvre auprès d'un office ou l'enregistrement des droits n'est pas nécessaire. Le dépôt légal est cependant pratiqué dans certaines législations. Par ailleurs, les idées ne peuvent être protégées que si elles sont fixées puisque seule la forme d'une œuvre est protégeable.

Les droits moraux concernent essentiellement la reconnaissance de la qualité d'auteur et le fait de décider si, quand, de quelle manière et sous quel nom son œuvre sera divulguée.

Les droits patrimoniaux concernent l'utilisation de l'œuvre (confection et vente d'exemplaires, présentation, mise en circulation, diffusion, etc.).

Le transfert de la propriété de l'œuvre, qu'il s'agisse de l'original ou d'une copie, n'implique pas celui de droits d'auteurs. Ceux-ci sont par ailleurs cessibles et transmissibles par succession.

Les droits voisins concernent les droits des artistes interprètes (personnes physiques qui exécutent une œuvre ou qui participent sur le plan artistique à l'exécution d'une œuvre), les droits de producteurs de phonogrammes ou de vidéogrammes ainsi que les droits des organismes de diffusion.

IV.1.3.3 Droit des marques

La marque a pour fonction de distinguer les produits et/ou services du titulaire de ceux d'autres entreprises. La marque a pour fonction d'identifier un objet (et non pas un sujet de droit identifié plutôt par un nom ou une raison de commerce).

Pour être susceptible de protection la marque ne doit pas correspondre aux:

- signes appartiennent au domaine public;
- formes qui constituent la nature même du produit et celles qui sont rendues nécessaires par la fonction de l'objet visé;
- signes propres à induire en erreur;
- signes contraires au droit en vigueur ou aux bonnes mœurs.

Pour être protégée, une marque doit être déposée. Une marque enregistrée peut faire l'objet d'une opposition si:

- elle est identique à une marque déjà enregistrée pour des produits identiques;
- elle est identique ou similaire à une marque déjà enregistrée pour des produits et/ou services identiques ou similaires lorsqu'il en résulte un risque de confusion.

IV.1.3.4 Droit des brevets

Les brevets d'invention sont délivrés pour les inventions nouvelles utilisables industriellement.

Les brevets d'inventions ne peuvent être délivrés ni pour ce qui découle d'une manière évidente de l'état de la technique, ni pour les variétés végétales ou les races animales, ni pour les procédés essentiellement biologiques d'obtention d'animaux ou de végétaux; cependant les procédés microbiologiques et les produits obtenus par ces procédés sont brevetables.

Le brevet est accordé (sous certaines conditions) à celui qui dépose la demande (inventeur, son ayant cause ou un tiers à qui l'invention appartient à un autre titre).

Si la même invention a été faite par plusieurs personnes de façon indépendante, le brevet appartient à celui qui peut invoquer un dépôt antérieur ou un dépôt jouissant d'une priorité antérieure.

IV.1.3.5 Protection intellectuelle d'un site web

Sur l'internet et particulièrement pour les sites web, il faut recourir à plusieurs droits pour protéger la propriété intellectuelle d'un site web[54]:

- Pour ce qui concerne le nom du domaine:
  - L'enregistrement du nom de domaine ne confère en tant que tel aucun droit exclusif spécifique à son titulaire.
  - Pour protéger un nom de domaine il faut se tourner du côté des bases légales que sont:
    - le droit des marques;
    - le droit des raisons de commerce;
    - le droit au nom;
    - le droit de la concurrence;
- Pour ce qui concerne le contenu du site:
  - La diffusion des œuvres sur l'internet:
    - le contenu crée spécialement pour le site, il est protégé par le droit d'auteur;
    - la numérisation d'une œuvre existante et sa diffusion en ligne est une forme de reproduction qui ne peut se faire sans le consentement de l'auteur de l'œuvre initiale;
    - les liens vers d'autres sites: la simple utilisation d'un lien hypertexte ne lèse aucun droit exclusif puisqu'elle n'entraîne aucune reproduction; la question est plus délicate pour les liens profonds (qui permettent d'arriver à une page sans passer par la page principale d'un site). Elle pose la question de savoir si la page en question est une œuvre ou pas! En général ce genre de litige se règle par le droit de la concurrence avec comme critère déterminant la manière dont les liens hypertextes sont utilisés, la loyauté de cet usage apparaît alors comme une notion centrale.

IV.1.3.6 Complémentarité des approches

Pour assurer le respect des droits d'auteurs, des mesures techniques se mettent en place. Les législations les soutiennent en interdisant de les contourner.

Ainsi il a la protection légale, la protection technique et la protection légale de la protection technique.

IV.1.4 Divers aspects juridiques liés au spam[55]

IV.1.4.1 Contexte et nuisances

Au sens large, le spam[56] désigne l'envoi de messages électroniques non sollicités. Il se caractérise ainsi:

- les messages non sollicités sont envoyés de manière massive et répétée;
- le message poursuit un objectif commercial ou est réalisé à des fins malveillantes (*phishing*, prise de contrôle de l'ordinateur, introduction de programme malveillant (virus, *adware*, *spyware*…));
- les adresses sont souvent obtenues à l'insu du propriétaire (en violation des règles relatives à la protection des données à caractère privé);
- le spam possède souvent un contenu illégal, trompeur ou préjudiciable.

---

54 Issu de Philippe Gilliéron; «Propriété intellectuelle et Internet» livre CEDIDAC 53, Université de Lausanne 2003.

55 Ce point à été élaboré en collaboration avec Igli Tashi, assistant diplômé de l'Université de Lausanne.

56 Le terme «SPAM» est à l'origine une marque déposée de la compagnie Hormel, et n'est autre que l'acronyme de «*Spiced Pork and Meat*», une sorte de corned-beef qui accompagnait les soldats américains durant la dernière guerre mondiale. Il semble que les Monty Python aient inspiré l'association de cet aliment avec la pratique d'envoi de courriels non sollicités. Ceux-ci, dans un de leurs célèbres sketches, se mettent à chanter «Spam Spam Spam Spam...» pour vanter les mérites du produit, de façon très répétitive et si fort que cela couvre les propos des autres protagonistes.

L'utilisation de spam dans certaines circonstances compte tenu de son caractère non sollicité peut être considérée comme une politique de vente ou de publicité agressive.

De nos jours le phénomène du spam ne se limite pas seulement à la messagerie électronique via l'internet mais aussi aux téléphones portables à travers les SMS ou aux nouveaux équipements multimédias comme les *pockets* PC.

Le spam génère des coûts pour tous les usagers de l'internet. Ces coûts sont généralement liés au temps de traitement des messages, à l'acquisition de différents outils pour se protéger contre ce phénomène sans compter le coût social c'est-à-dire une perte de confiance de la part des utilisateurs, une baisse de productivité des organisations, etc.

Selon une étude de la société Clerswift publiée par le *Journal du Net* le 13 septembre 2005, la répartition du spam selon les catégories suivantes est:

Types de spam	juin 2005
Santé	43.86%
Produits	37.65%
Finance	9.06%
Pornographie	5.32%
Phishing	1.41%
Pari	0.1%
Autres	2.32%

Le spam peut prendre la forme de diverses escroqueries dont une des plus communes est celle dite escroquerie nigérienne ou *Nigerian letter*[57]. Le *phishing* consiste à envoyer un message semblant être émis par une institution connue comme une banque par exemple, qui invite sous divers prétextes, l'internaute à se connecter sur un site contrefait d'une institution visée et à donner ses codes d'accès et informations sensibles, qui seront utilisées ultérieurement à son insu.

Outre les escroqueries et le *phishing*, le spam peut aussi être envoyé dans un but destructeur et de blocage de la messagerie du destinataire occasionnant ainsi indisponibilité et déni de service des ressources. Le «bombardement» de messages peut prendre diverses formes: envoi de messages de grandes tailles générant des problèmes au niveau du traitement ou du stockage temporaire, envoi de grands nombres de messages ou envoie à un nombre très important de destinataires dans le but d'inonder le serveur, ou encore, usurpation de l'adresse de l'émetteur.

IV.1.4.2 Réponses juridiques au phénomène du spam

Le spam relève de plusieurs domaines juridiques, notamment, la protection des données, la concurrence déloyale mais aussi le domaine pénal.

---

[57] L'émetteur du spam se présente comme l'héritier d'un riche notable, parfois dans un pays lointain, récemment décédé. Le soi-disant héritier prétend avoir des difficultés pour faire valoir ses droits et propose à la victime d'utiliser le compte en banque de cette dernière et lui propose en échange une rémunération importante pour la gêne occasionnée. Cette dernière doit avancer les frais relatifs à la transaction. Ce sont invariablement des tentatives d'escroquerie.

Exemple suisse

En Suisse, aucune norme juridique suisse ne règle explicitement la question du spam.

D'un point de vue de la protection des données, selon le Préposé Fédéral à la Protection des données et son document «*Aide-mémoire concernant les messages publicitaires indésirables diffusés par courrier électronique (spams)*»[58] précise que «*les adresses électroniques constituent des données personnelles permettant d'identifier une personne».* Conformément à l'art. 12, al. 3, de la loi fédérale suisse, sur la protection des données (LPD, RS 235.1), «…*En règle générale, il n'y a pas atteinte à la personnalité lorsque la personne concernée a rendu les données accessibles à tout un chacun et ne s'est pas opposée formellement au traitement*.». Le traitement d'adresses électroniques par un spammeur constitue un détournement du but premier si on considère l'art. 4, al. 3, LPD, commis à l'insu art. 4, al. 2, LPD et sans le consentement art. 13, al. 1, LPD de la personne concernée. Il s'agit donc bien d'une atteinte à la protection des données.

Art. 4 Principes

[1] Toute collecte de données personnelles ne peut être entreprise que d'une manière licite.

[2] Leur traitement doit être effectué conformément aux principes de la bonne foi et de la proportionnalité.

[3] Les données personnelles ne doivent être traitées que dans le but qui est indiqué lors de leur collecte, qui est prévu par une loi ou qui ressort des circonstances.

La loi sur la protection des données donne aux personnes concernées la possibilité d'agir en justice art. 15 LPD basé sur l'art. 28 ss du CC.

Directive européenne

Au niveau européen la directive 95/46/CE du 24 octobre 1995 *relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel* donne les standards minimaux ne matière de constitution de fichiers et de traitement de données. L'art. 10 de cette directive impose que le titulaire connaisse la finalité de la collecte et l'identité du contrôleur.

Exemple de la France

En France. La loi «informatiques et libertés» a inséré dans le Code pénal français l'infraction des atteintes au droit de la personne résultant des fichiers ou des traitements informatiques. Cette loi datant de 1978 a été revue en 2004 en introduisant 14 nouveaux articles durcissant les peines concernant les donnés à caractère personnel.

Exemple des Etats-Unis

Les Etats-Unis étant le premier pays générateur du spam, s'est doté d'un texte de loi spécifique concernant le spam, permettant de poursuivre les *spammers*, le CAN SPAM Act du 1er janvier 2004.

La collecte des adresses sur des sites web est interdite et sont prohibés les programmes qui génèrent des adresses en combinant aléatoirement des lettres et des chiffres.

Le spam pose aussi un problème du point de vue de la concurrence déloyale du fait que le spam soit utilisé dans un but publicitaire.

Spam, publicité et concurrence déloyale

La publicité sur l'internet ne dispose pas d'un cadre légal spécifique. Elle se réfère au droit de la publicité en général. En novembre 2001, la Commission suisse pour la loyauté avait rendu un avis relatif au spamming, le considérant comme une méthode de vente particulièrement agressive. L'utilisation d'une telle méthode vu sous l'angle de la publicité doit respecter quelques aspects importants que ce soit dans le cadre du commerce «classique» aussi bien que dans celui du e-commerce.

---

[58] Site: www.edsb.ch/f/doku/merkblaetter/spam.htm

Cela concerne:

- la protection des jeunes internautes;
- le respect de la personne humaine;
- le respect d'une publicité loyale, véridique et honnête;
- le respect de l'intimité juridique des internautes;
- le confort de la navigation.

Le législateur suisse dans sa loi fédérale contre la concurrence déloyale stipule à l'article 3, lettre b, c, d,: *«Agit de façon déloyale celui qui, notamment:*

……

b. Donne des indications inexactes ou fallacieuses sur lui-même, son entreprise, sa raison de commerce, ses marchandises, ses œuvres, ses prestations, ses prix, ses stocks, ses méthodes de vente ou ses affaires ou qui, par de telles allégations, avantage des tiers par rapport à leurs concurrents;

c. Porte ou utilise des titres ou des dénominations professionnelles inexacts, qui sont de nature à faire croire à des distinctions ou capacités particulières;

d. Prend des mesures qui sont de nature à faire naître une confusion avec les marchandises, les œuvres, les prestations ou les affaires d'autrui».

Mais c'est notamment dans sa lettre h qu'il touche le cœur de la problématique du spam en stipulant que:

«Agit de façon déloyale celui qui, notamment:

……

h. Entrave la liberté de décision de la clientèle en usant de méthodes de vente particulièrement agressives»

Utilisé dans un but commercial avec l'intensité de l'envoi observé, l'utilisation du spam peut tomber sur le coup de cet article.

Spam et intention criminelle

Lorsque les spammeurs agissent avec une intention criminelle, cette dernière peut être placée sur le plan du droit pénal. Même si les messages peuvent revêtir un caractère commercial, le contenu peut faire objet de poursuites.

Spam et pornographie

La majorité des messages de spams invitent à visiter des sites pornographiques. Cette action est réprimée par l'art. 197 du CPS (Code pénal suisse), notamment le fait de rendre accessible ce genre de contenu à des personnes qui n'en veulent pas (art.197, al.2) et aux personnes qui ont moins de 16 ans (art.197, al.1).

Spam, escroquerie, virus et vente de produits prohibés

L'escroquerie est réprimée par l'art. 146 du Code pénal suisse. Il s'agit du fait d'obtenir de la victime et dans un dessein d'enrichissement un avantage pécuniaire. Ce raisonnement peut tout à fait être appliqué dans le cas de la lettre nigérienne.

Le spam est parfois le meilleur moyen d'introduire des virus dans les machines destinataires. En droit suisse l'introduction de virus serait considérée comme une détérioration de données et réprimé ainsi par l'art.144bis du Code pénal, pour autant que ce virus ait provoqué des dégâts (modification, effacement ou mise hors usage des données) chez l'internaute touché.

Le fait d'utiliser les spam dans un but de vente des médicaments est aussi une pratique prohibée par la loi suisse. La loi sur les médicaments et les dispositifs médicaux (LPTh) et son art. 32 prohibe la publicité pouvant inciter à un usage excessif, abusif ou inapproprié de médicaments ou la publicité pour les médicaments qui ne peuvent être mis sur le marché en Suisse et qui ne peuvent être remis que sur ordonnance.

IV.1.4.3 Régulation du Spam

Deux visions s'opposent pour la régulation du spam: l'*opt-in* et l'*opt-out*.

L'*opt-in*, également appelée «*permission marketing*», est la plus respectueuse de l'internaute dans la mesure où elle consiste à ne lui envoyer des publicités ciblées que s'il y a explicitement consenti. Le choix de recevoir des messages publicitaires peut être proposé sous forme de case à cocher, à décocher ou encore être induit. Dans ce dernier cas, le visiteur doit être clairement prévenu du caractère commercial et des conséquences exactes de son inscription.

La notion d'*opt-out* fait référence à la «désinscription» et consacre l'existence d'un droit d'opposition *a posteriori* de recevoir des courriers électroniques. A cet effet, chaque message publicitaire envoyé doit offrir la possibilité de se désinscrire du fichier. Les fichiers *opt-out* peuvent aussi bien être constitués de manière légale (par exemple d'un achat d'un fichier *opt-in*) qu'issus d'une collecte sauvage.

Le législateur suisse et américain ont optés pour la solution de *opt-out* tandis que la démarche communautaire européenne penche plutôt vers la solution de *opt-in* se basant à la directive 2002/58/CE *concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques.*

Etant donné que le spammeur agit souvent sous le couvert de l'anonymat ou depuis l'étranger, la poursuite en justice se révèle onéreuse et compliquée et implique la plupart du temps le recours à un avocat.

IV.1.4.4 Réponses techniques au phénomène du spam

Techniques basées sur la limitation des ressources

En limitant les ressources comme le nombre de destinataires par message, le nombre de messages par source et par unité de temps pourrait limiter l'impact du spam.

Liste noire

Le principe est de qualifier le courrier en fonction de la réputation du serveur qui l'a émis.

La réputation d'un serveur de courrier qui a émis du spam récemment est entachée, dans la mesure où l'on suppose qu'il pourrait à nouveau en émettre. Le serveur émetteur est identifié par son adresse IP.

Filtre à base de mots clés

Il s'agit de filtrer les messages selon certains mots clés. Cette technique est insuffisante, car il est très aisé pour un spammeur d'avoir un contenu de messages qui contourne les filtres à mots clés.

Filtre à empreinte

Dans la mesure ou le spam consiste en l'envoi massif de messages tous identiques, un filtre à empreinte calcule une signature du contenu d'un courriel et le compare à une base de données d'empreinte de messages considérés comme du spam.

Politique de lutte contre les logiciels malveillants

De plus en plus de logiciels malveillants (virus, chevaux de Troie, *bot*,...) installent un serveur de messagerie sur la machine qu'ils ont compromise. Cette fonctionnalité des outils malveillants est destinée à faciliter la propagation du spam. Lutter contre le spam, passe aussi par la chasse aux logiciels malveillants.

L'utilisation des logiciels anti-spams au niveau des serveurs de messagerie contribuent à limiter la propagation du spam en le bloquant, ne sont pas toujours efficaces. En effet, les messages qui ne sont pas des spams ne parviennent pas aux destinataires (notion de *faux négatifs*) ou encore, les messages réellement de spam sont considérés comme normaux (notion de des *faux positifs*).

De plus, le comportement de l'internaute peut avoir aussi un rôle important dans la lutte anti-spam. Ainsi par exemple, l'adoption d'un comportement averti de la messagerie (sensibilisation au risque d'usurpation d'identité, contrôle préalable de l'usage qui sera fait de son adresse électronique avant de le confier à un formulaire en ligne, l'utilisation de plusieurs adresses électroniques, éviter certains sites, ne pas ouvrir de message dont on ne connaît pas l'origine, supprimer des messages de spam sans les lire, ne jamais répondre, ne jamais cliquer sur les liens hypertextes que ces messages comportent…) contribue à l'imiter l'ampleur du spam.

IV.1.4.5 Complémentarité technico-juridique

Dans la mesure où le volet juridique a un impact limité sur la pratique du spam, une solution d'ordre technologique s'impose. Seule la complémentarité des approches technico-juridiques permet de lutter contre le phénomène du spam. Un spammeur de moins, découragé par une règle de droit ou empêché efficacement par une solution technique, présente toujours des millions et des millions de *spams* non envoyés.

IV.1.5 Récapitulatif des principaux problèmes juridiques liés au cyber espace[59]

IV.1.5.1 Statut juridique de l'internet marchand

Le statut juridique de l'internet marchand concerne la définition des statuts des outils utilisés dans le cadre de l'utilisation des technologies de l'information.

Pour ce qui concerne la messagerie électronique: des questions se posent concernant le contenu des messages, l'adresse de messagerie, la problématique de l'identification à travers cette adresse: usurpation d'identité, d'un signe distinctif, d'une raison sociale d'une entreprise. Cela relève du droit civil des pays.

Pour ce qui concerne un site web: la notion d'œuvre, sa qualification audiovisuelle ou non, soulèvent des problèmes liés au droit d'auteur. Un lien hypertexte renvoie au problème de son contenu, de la responsabilité, de la qualification protégée ou non et soulève également des problèmes liés aux moteurs de recherche.

IV.1.5.2 Cybercontrat

Réaliser des contrats dans le cyberespace ne pose pas uniquement un problème d'ordre juridique. En effet, cela nécessite entre autre, la mise en place de mécanismes techniques qui permettent de le réaliser (outils et procédés utilisés (globalité, incorporalité, délocalisation)).

D'un point de vue juridique, retenons:

- l'offre; qualification (à distance ou pas), acceptation;
- la publicité et le démarchage, le spam etc.
- l'exécution de contrat;
- l'acceptation de l'offre *on line* et l'expression informatique de l'acceptation;
- le droit de rétractation;
- la détermination de la loi applicable ainsi que des juridictions compétentes

Diverses directives européennes y sont relatives, à savoir:

- le Règlement de CE 44/2001 du 22 décembre 2000 concernant la compétence juridictionnelle, la reconnaissance des décisions en matière civile et commerciale);
- la Directive CE 2000/31 sur le commerce électronique;

---

59 Ce point à été élaboré en collaboration avec Igli Taschi, assistant diplômé à l'Ecole des HEC de l'Université de Lausanne.

- La Directive 98/34/CE qui prévoit une procédure d'information dans le secteur des normes et des réglementations techniques;
- La Directive 97/7/CE du Parlement européen et du Conseil, du 20 mai 1997, concernant la protection des consommateurs en matière de contrats à distance

De plus, il faut tenir compte de la loi de CNUDCI sur le commerce électronique 1996, des *declarations on the global Electronic Commerce* 1998, du *Joint EU-US statement on Electronic commerce*

IV.1.5.3 Document et signature électronique

Le document électronique signé électroniquement soulève le problème de sa valeur. L'objectif étant de pouvoir garantir la valeur juridique de la signature apposée sur un document afin d'identifier l'auteur et de constater la volonté d'apposer la signature et donc d'assumer la responsabilité du contenu du document.

Rappelons la Directive CE 93/1999 du 13 décembre 1999 relative à une cadre communautaire pour les signatures électroniques et en *Italie,* la loi du 15 mars 1997 n° 59, aux USA, *Electronic Signatures in Global et National Commerce Act* du 30 juin 2000 ainsi qu'en Grande-Bretagne par exemple *Electronic Communication Act* du 25 mai 2000.

IV.1.5.4 Moyens de paiement électronique

Les moyens de paiement électronique, cartes de crédit, chèques ou monnaie électronique peuvent induire une utilisation abusive de la part de tiers qui arrivent à intercepter l'information associée, lors par exemple de la communication entre fournisseurs et destinataires de service.

La Directive CE 2000/46 sur la monnaie électronique

IV.1.5.5 Protection des noms de domaine

Un nom de domaine constitue un nouveau bien incorporel qui peut posséder une valeur commerciale considérable. La problématique associée au nom de domaine relève des points suivants:

- Marques et noms de domaine
- Signes distinctifs et noms de domaine
- Nom commerciaux et noms de domaine

A part les lois nationales sur le marques, les noms, les brevets, retenons aux Etats-Unis la loi Anticybersquatting Consumer Protection Act (ACPA)

IV.1.5.6 Propriété intellectuelle

La propriété intellectuelle sur internet relève des problématiques liées aux droits d'auteur, aux maques et aux brevets. Retenons par exemple: le traité de l'OMPI sur les droits de l'auteur, le traité de l'OMPI sur les interprétations, exécutions et phonogrammes, au niveau européen le livre vert sur le droit d'auteur et les droits connexes dans la société de l'information de 1995 ainsi que la directive du parlement européen et du conseil sur l'harmonisation de certains aspects du droit d'auteur et du droit connexe dans la société de l'information.

IV.1.5.7 Protection de l'intimité numérique

Dans le contexte de la protection de l'intimité numérique, le spamming est prohibé (Cf. Directive EU 97/7 sur la protection des consommateurs dans les contrats conclus à distance, Directive CE 97/66 sur la protection des personnes à l'égard des données personnelles dans le domaine des télécommunications interdit le direct marketing du spam).

IV.1.5.8 Autres questions d'ordre juridique

Sans vouloir être exhaustif, de nombreuses autres questions juridiques doivent être prises en considération lors que l'on s'intéresse à la définition d'un cadre légal approprié à l'usage de l'internet. Parmi elles retenons toutes celles qui touchent:

- à la notion d'antitrust (Cf. les directives américaines «*Antitrust guidelines for collaboration among competitors*» d'avril 2000*);*
- à la responsabilité des fournisseurs et intermédiaires techniques (quelles responsabilités pour le fournisseur concernant les activités de l'internaute, les activités criminelles, la pedo-pornographie etc.);
- au secret des correspondances.

Chapitre IV.2 – Perspectives

IV.2.1 Eduquer – former – sensibiliser l'ensemble des acteurs à la cybersécurité

Il est important de sensibiliser l'ensemble des acteurs du monde de l'internet aux enjeux de la maîtrise de la sécurité et aux mesures élémentaires qui si elles sont clairement énoncées, définies et mise en œuvre intelligemment renforceront la confiance des utilisateurs envers les technologies de traitement de l'information et de la communication dont fait partie l'internet. Faisons de ce dernier, un patrimoine ouvert à chacun et non au bénéfice exclusif de la criminalité.

La diffusion d'une certaine culture et approche pluridisciplinaire de la sécurité et de la maîtrise du risque informatique d'origine criminel est obligatoire. Posséder une vision stratégique de ces problématiques est devenue une nécessité pour les organisations comme pour les Etats.

Par ailleurs, il également nécessaire d'éduquer, d'informer et former aux technologies de traitement de l'information et des communications et non uniquement à la sécurité et aux mesures de dissuasion. La sensibilisation aux problématiques de sécurité ne doit pas se limiter à la promotion d'une certaine culture de la sécurité. En amont de la culture sécuritaire, il doit y avoir une culture de l'informatique. Il faut aussi donner les moyens aux différents acteurs d'apprendre à gérer les risques technologique, opérationnel et informationnel qui les menacent en fonction de l'usage fait des nouvelles technologies.

La dimension virtuelle de l'internet, son côté ludique, peut occulter – notamment pour un public jeune, ou non initié à l'informatique – la capacité de nuisance de ces attaques. Elle est considérable et peut s'avérer dramatique tant pour les organisations (entreprise, administration, collectivité), que les individus qui en sont victimes. Toutefois, la maîtrise des risques technologiques ne se résume pas à la chasse aux *hackers*, ni à la mise en place de barrière technologiques. Les dégâts les plus graves ont parfois pour origine une simple négligence, qui peut relever de l'incompétence, des défaillances lors de la conception ou de la mise en œuvre des technologies, des pouvoirs excessifs accordés aux administrateurs systèmes, d'une gestion défectueuse, etc.

IV.2.2 Pour une nouvelle approche de la sécurité

La prise de conscience de la fragilité du monde numérique et de la non maîtrise totale non seulement des technologies et infrastructures informatiques et télécoms mais aussi des solutions de sécurité commercialisées, doit soulever un questionnement sérieux quand à la dépendance vis-à-vis d'une technologie difficilement maîtrisable. La prise en otage des données par des solutions informatiques est une réalité qu'il ne faut pas occulter.

Il est illusoire de penser que des solutions d'ordre technologiques ou juridiques viendront suppléer les erreurs de conception et de gestion de l'informatique et des télécoms, que cela soit au niveau stratégique, tactique ou opérationnel. De plus, les mesures classiques de sécurité ne pourront protéger correctement les ressources sensibles ou critiques des personnes, des organisations et des Etats, uniquement si elles sont réalisées de manière transparente, vérifiables et contrôlable.

Mettre en place une démarche complète de sécurité qui intègre des phases de prévention, de protection, de défense et de réaction, passe par l'adoption de moyens humains, juridiques, technologiques, économiques permettant de les réaliser.

IV.2.3 Propriétés d'une politique de sécurité

De manière générale, une bonne politique de sécurité résulte d'une analyse des risques et est définie de manière complète et cohérente, afin de répondre précisément aux besoins de sécurité dans un contexte donné.

La définition de la politique doit être:

- simple et compréhensible;
- adoptable par un personnel préalablement sensibilisé, voire formé;
- aisément réalisable;
- de maintenance facile;
- vérifiable et contrôlable.

Une politique de sécurité ne doit pas être statique. Elle doit être périodiquement évaluée, optimisée et adaptée à la dynamique du contexte dans lequel elle s'inscrit. Elle doit être configurable et personnalisable selon des profils d'utilisateurs, selon les flux, en fonction du contexte et de la localisation des acteurs en jeu. Une politique de sécurité varie en fonction de l'espace et du temps.

Une politique de sécurité peut être structurée en différentes politiques de contrôle d'accès, de protection, de gestion de crise, de suivi et d'optimisation, d'assurance.

IV.2.4 Identifier les ressources sensibles afin de les protéger

La réalisation d'un inventaire complet et précis de toutes les ressources et acteurs de la chaîne sécuritaire, contribue à la connaissance des environnements ainsi qu'à leur protection. L'identification des valeurs et la classification des ressources pour déterminer leur degré de sensibilité (ou degré de criticité) permet de différencier ce qui doit être impérativement êtresécurisé. Ce dernier indique leur importance en cas de perte, d'altération ou de divulgation des données. Plus les conséquences sont graves pour l'organisation, plus la ressource est sensible et possède de la valeur.

Chaque ressource peut être perçue comme une cible de sécurité pour laquelle, il faut identifier les risques et leurs scénarios possibles (erreur d'utilisation, de paramétrage, accidents, malveillance, sabotage, attaque logique, etc.), les mécanismes de sécurité inhérents et applicables (configuration, paramètres, etc.), ainsi que les contraintes techniques et organisationnelles afin de déterminer la faisabilité technique et organisationnelle de la politique de sécurité pour chaque cible.

IV.2.5 Objectifs, mission et principes fondamentaux de la cybersécurité

Les objectifs de la cybersécurité sont:

- la confidentialité (aucun accès illicite): maintien du secret de l'information et accès aux seules entités autorisées;
- l'intégrité et l'exactitude (aucune falsification, aucune erreur): maintien intégral et sans altération des données et programmes;
- la disponibilité (aucun retard): maintien de l'accessibilité en continu sans interruption, ni dégradation;
- la pérennité (aucune destruction): les données et logiciels existent et sont conservés le temps nécessaire;
- la non-répudiation et l'imputabilité (aucune contestation): garantie de l'origine, de la source, de la destination, de la véracité d'une action;
- le respect de l'intimité numérique;
- l'authentification (aucun doute sur l'identification d'une ressource).

Les activités d'une mission peuvent se décliner selon les axes suivants:

- concevoir un plan de sécurité en fonction d'une analyse préalable des risques;
- définir le périmètre de vulnérabilité lié à l'usage des nouvelles technologies;
- offrir de manière continue un niveau de protection adapté aux risques encourus;
- mettre en œuvre et valider l'organisation, les mesures, les outils et les procédures de sécurité;
- effectuer un suivi, auditer, contrôler, faire évoluer le système d'information et sa sécurité;
- optimiser la performance du système d'information en fonction du niveau de sécurité requis;
- aligner les besoins avec les risques et les coûts.

Les principes fondamentaux auxquels doit se référer toute action entreprise au nom de la réalisation de la cybersécurité sont les suivants:

- principe de vocabulaire. Nécessité de s'accorder sur un langage commun de définition de la sécurité;
- principe de cohérence. La cybersécurité résulte de l'intégration harmonieuse des outils, mécanismes et procédures liés à la prévention, à la détection, à la protection et à la correction des sinistres relatifs à des fautes, à la malveillance ou à des éléments naturels;
- principe de volonté directoriale. Il est de la responsabilité des dirigeants de libérer les moyens nécessaires à la mise en œuvre et à la gestion d'un plan de cybersécurité;
- principe financier. Le coût de la sécurité, des mesures de contrôle, doit être en rapport avec le risque;
- principe de simplicité, d'universalité et de discrétion. Les mesures de sécurité doivent être simples, souples, compréhensibles pour les internautes. Les solutions et mesures de sécurité ne doivent pas être provocantes afin de ne pas tenter un attaquant potentiel;
- principe de dynamicité et de continuum. La sécurité doit être dynamique pour intégrer la dimension temporelle de la vie des systèmes et de l'évolution des besoins et des risques. Les systèmes doivent être opérationnels de manière permanente;
- principe d'évaluation, de contrôle et d'adaptation afin d'assurer l'adéquation du niveau de sécurité aux besoins réels.

IV.2.6 Facteurs de réussite

IV.2.6.1 Lignes directrices en matière de stratégie

Les conditions de succès de la réalisation d'une stratégie sécuritaire sont:

- une volonté stratégique
- une politique de sécurité simple, précise, compréhensible et applicable;
- la publication de la politique de sécurité;
- une gestion centralisée de la sécurité et une certaine automatisation des processus de sécurité;
- un niveau de confiance et d'intégrité des personnes, des systèmes, des outils impliqués;
- des procédures d'enregistrement, de surveillance et d'audit;
- la volonté d'éviter de mettre les ressources en situation dangereuse;
- un cadre légal applicable au niveau national et international;
- le respect des contraintes légales.

IV.2.6.2 Lignes directrices à l'usage des internautes

Voici quelques lignes directrices à l'intention des internautes qui constituent des mesures simples, économiques et relativement efficaces, que si elles sont adoptées par les utilisateurs, contribueront à renforcer la sécurité de leur ressources et e-activités[60]:

- L'ordinateur lorsqu'il n'est pas utilisé doit être éteint;
- L'internaute ne doit pas ouvrir les mails dont il ne connaît pas la provenance;
- L'internaute doit avoir un antivirus mis à jour régulièrement afin d'assurer une sécurité minimale;
- L'internaute ne doit pas divulguer ses mots de passe et il doit les changer régulièrement;
- L'internaute ne doit pas divulguer de données personnelles le concernant lui ou les autres sur l'internet;
- L'internaute ne doit pas permettre à une autre personne d'utiliser son compte pour surfer sur l'internet;
- L'internaute doit utiliser les systèmes de chiffrement lorsqu'il veut protéger ses données;
- L'internaute ne doit pas aller sur des sites à caractère choquant, télécharger des programmes ou fichiers illégaux ou encore les faire circuler;
- Ce que l'internaute ne fait pas dans la vie réelle, il ne doit pas le faire sur le web sous peine d'être punissable (diffamation, escroquerie, etc.);
- L'internaute ne doit pas se sentir plus protégé qu'il ne l'est réellement;
- L'internaute doit garder présent à l'esprit que derrière chaque activité sur l'internet se cache un individu qui, à l'image de la vie courante, n'est pas forcément honnête.

IV.2.6.3 Lignes directrices pour sécuriser un système de messagerie

Voici quelques lignes directives élémentaires qui contribuent à protéger un système de messagerie.

Du côté du serveur:

- implanter un logiciel anti-virus;
- filtrer les messages sur certains critères paramétrables (taille, fichiers attachés, etc.);
- configurer correctement le serveur;
- effectuer une gestion efficace pour en assurer la disponibilité;
- éviter les comptes de maintenance par défaut;
- assurer une protection physique du serveur.

Du côté de l'utilisateur:

- installer, gérer et imposer l'usage de logiciels anti-virus;
- définir des règles d'utilisation de la messagerie (ne pas ouvrir des fichiers exécutables, etc.);
- sensibiliser suffisamment les utilisateurs aux risques encourus;
- faire s'engager les utilisateurs sur un usage approprié des ressources informatiques;
- configurer correctement le poste de travail de l'utilisateur et son application de messagerie;
- implanter des versions de messagerie sécurisées;
- utiliser des procédures de chiffrement pour les messages confidentiels et réaliser l'authentification des sources.

---

60 Issues du travail de mémoire de DEA en Droit, Criminalité et Sécurité des nouvelles technologies. «Sentiment de sécurité sur Internet» Anne-Sophie Perron, sous la direction de S. Ghernaouti-Hélie – Lausanne 2005.

IV.2.6.4 Lignes directrices pour protéger un environnement internet-intranet

Voici quelques lignes directives élémentaires qui contribuent à protéger un environnement internet-intranet, via un système pare-feu (firewall):

- un firewall doit être protégé et sécurisé contre des accès non autorisés (notion de système de confiance possédant un système d'exploitation sécurisé);
- tous les trafics (entrants et sortants) doivent passer par le firewall;
- seul le trafic défini par la politique de sécurité comme étant valide et autorisé peut traverser le firewall;
- configurer le firewall de telle sorte que tout ce qui n'est pas explicitement autorisé est interdit;
- un firewall ne peut également être le serveur Web de l'entreprise;
- si les données du réseau interne sont vraiment sensibles, il faut alors accéder à l'internet par des machines détachées du réseau interne;
- un firewall ne peut pas protéger l'environnement à sécuriser contre des attaques ou des accès illicites qui ne passent pas par lui. Il n'est d'aucune efficacité en ce qui concerne des délits perpétrés à l'intérieur de l'entreprise;

Un firewall n'est pas un anti-virus. Il faut donc le protéger de manière complémentaire contre des infections virales. Dans l'absolu, un anti-virus devrait résider sur tous les systèmes offrant un service de connectivité (serveurs de messagerie, serveur de communication, etc.) et sur toutes les machines supportant des données (serveur d'archivage, de bases de données, etc.), ainsi que sur les postes de travail des utilisateurs.

SECTION V

ANNEXES

Annexe A – Glossaire des principaux termes de sécurité[61]

Accident (*accident*)

Elément fortuit, imprévisible portant atteinte à une entité.

Administrateur de la sécurité (*security administrator*)

Personne responsable de la définition ou de la réalisation de tout ou partie d'une politique de sécurité.

Algorithme cryptographique (*cryptographic algorithm*)

Algorithme utilisé pour le chiffrement des données afin de les rendre confidentielles, il est basé sur une fonction mathématique et une clé de chiffrement.

Algorithme de cryptographie asymétrique (*asymmetric cryptographic algorithm*)

Algorithme basé sur l'usage d'une bi-clé, l'une servant au chiffrement des données, l'autre au déchiffrement.

Analyse de risque (*risk analysis*), ***évaluation des risques*** (*risk assessment*)

Processus d'identification et d'évaluation des risques (estimation de leur probabilité d'occurrence et de leurs impacts).

Analyse du trafic (*traffic analysis*)

Observation et étude des flux d'information entre entités source et destination (présence, absence, volume, direction, fréquence, etc.).

Anonymat (*anonymity*)

Caractéristique d'une entité dont on ignore le nom, ou qui ne fait pas connaître son nom, propriété permettant à une entité d'utiliser des ressources sans être identifiée (incognito). Il devrait être possible de respecter la volonté de certains utilisateurs qui peuvent avoir une raison valable de ne pas révéler leur identité lorsqu'ils font des déclarations sur l'internet afin de ne pas restreindre de manière excessive leur liberté d'expression, favoriser l'expression libre d'informations et d'idées et d'assurer une protection contre les surveillances en ligne non autorisée par des entités publiques ou privées. En revanche, les instances de justice et de police devraient avoir la possibilité d'obtenir des informations sur les personnes responsables d'activités illicites, dans les limites fixées par le droit national, la Convention européenne des Droits de l'Homme, et les autres traités internationaux comme la Convention sur la cybercriminalité.

Antivirus

Programme de détection de virus.

Attaque (a*ttack*)

Offensive, agression, action contre des personnes ou des biens leur portant atteinte. Il existe différents types d'attaques informatiques.

---

61 Issu et adapté du glossaire du livre «Sécurité informatique et réseaux, cours et exercices corrigés»; S. Ghernaouti-Hélie, Dunod 2006.

Attaque active (*active attack*)

Attaque qui modifie les ressources ciblées par l'attaque (atteinte aux critères d'intégrité, disponibilité, confidentialité).

Attaque passive (*passive attack*)

Attaque qui n'altère pas sa cible (écoute passive, atteinte à la confidentialité).

Atteinte (*breach*)

Effet ou dégradation résultant d'une agression, d'une attaque qui peut avoir des *impacts tangibles* (altération physique et matérielle, dysfonctionnement logique, désorganisation des procédures...); des *impacts logiques* (non-disponibilité, perte d'intégrité, perte de confidentialité de l'information); des *impacts stratégiques* (notamment sur le plan financier, frais supplémentaires d'hébergement, de transport, de télécommunications, d'intervention d'experts, d'achat/location de matériel et progiciels, de personnels, et de sous-traitance, pertes d'exploitation (pertes de marge, de trésorerie, de clientèle), de fonds ou de biens, etc.).

Audit de sécurité (*security audit*)

Examen méthodique de toutes les composantes et acteurs de la sécurité, politique, mesures, solutions, procédures et moyens mis en œuvre par une organisation, pour sécuriser son environnement, effectué à des fins de contrôle de conformité, d'évaluation de l'adéquation des moyens (organisationnel, technique, humain, financier) investis au regard des risques encourus, d'optimisation, de rationalité et de performance.

Auditabilité (*auditability*)

Propriété pour un environnement, de permettre l'enregistrement des actions, d'événements qui occurrent afin de laisser une trace exploitable à des fins d'analyse et d'audit.

Auditeur (*auditor*)

Personne réalisant un audit.

Authenticité (*authenticity*)

Caractère de ce qui est authentique. Capacité permettant d'attester, de certifier conforme à... . Souvent associé au fait qu'une information, ou qu'un événement n'ait pas été altéré, modifié, contrefait et qu'il ait été produit par l'entité qui revendique les avoir réalisés.

Authentification (*authentication*)

Action d'authentifier. L'authentification sert à confirmer (ou non) qu'une action, déclaration, information est authentique (originale, vraie). Processus mis en œuvre notamment pour vérifier l'identité d'une entité et s'assurer que l'identité fournie correspond à l'identité de cette entité préalablement enregistrée.

Autorisation (*authorization*)

Action d'autoriser, de permettre, d'habiliter. Fait de recevoir la permission à réaliser certaines actions, d'accorder des droits, d'obtenir le droit d'accès à un service, à des informations, à un système, etc.

Autorité (*authority*)

Organe du pouvoir. Fait référence le plus souvent à une entité responsable de l'émission des certificats numériques.

Autorité de certification (CA, *Certification Authority*)

Tierce partie de confiance pour la génération, la signature et la publication des certificats de clés publiques.

Besoin de sécurité (*security need*)

Pour un environnement à protéger, identification et expression des niveaux de disponibilité, d'intégrité et de confidentialité associés aux ressources et valeurs faisant l'objet de la protection.

Bien, valeur (*asset*)

Entité qui a un prix et qui représente pour celui qui la possède un capital, un patrimoine (notion de *bien sensible*). En matière de sécurité il est important de déterminer les valeurs et de les classifier en fonction de leur importance, afin de mettre en place les mesures de protection nécessaires et suffisantes afin d'éviter de les perdre ou du moins de minimiser les impacts négatifs consécutifs à leur perte éventuelle.

Bogue (*bug*)

Terme d'origine anglaise qui illustre une erreur de programmation. Par extension défaut de conception ou de réalisation se manifestant par des anomalies de fonctionnement (J. O. 19 février 1984).

Bombe logique (*logical bomb*)

Programme malveillant qui s'active lors de la réalisation d'événements particuliers (date anniversaire par exemple) pour porter atteinte au système dans lequel il se trouve.

Certificat (*certificate*)**, certificat de clé publique** (*public-key certificate*)

Ensemble des données émises par une autorité de certification (tiers de confiance) qui permet de réaliser des services de sécurité (confidentialité, authentification, intégrité). Un certificat dit numérique fait référence à la mise en œuvre du chiffrement à clé public. En effet, dans un certificat se trouve entre autres la valeur de la clé publique de son propriétaire qui est attestée par le fait que le certificat est signé par l'autorité de certification émettrice.

Charte d'utilisation (*user charte*)

Document établi par une organisation précisant les droits, les devoirs et la responsabilité de ses employés au regard de l'utilisation des ressources informatiques et télécoms qu'elle met à leur disposition, signé par les parties concernées.

Cheval de Troie (*Troyan horse*)

Programme malveillant introduit subrepticement dans des systèmes pour en prendre le contrôle (vol de temps processeur, altération, modification, destruction des données et programmes, dysfonctionnements, écoutes illicites, etc.).

Chiffrement, cryptage, encodage (*encipherment, encryption*)

Le chiffrement est une transformation cryptographique des données (*cryptogramme*) afin d'en assurer la confidentialité. Cela consiste à rendre les données incompréhensibles à tous ceux qui ne détiendraient pas la clé de déchiffrement. Un texte en clair est chiffré à l'aide d'un algorithme et d'une clé de chiffrement, afin d'obtenir un texte chiffré, qui pourra être déchiffré à l'aide d'une clé de déchiffrement correspondante (sauf dans le cas où le chiffrement est irréversible). Le *déchiffrement* (*decipherment, decryption*) est l'opération inverse au chiffrement.

Clé (*key*)

Clé de chiffrement ou de déchiffrement, il s'agit généralement d'une valeur mathématique fournie à un algorithme de chiffrement. Sauf s'il s'agit d'une clé publique, une clé de chiffrement est à gérer comme un secret. Ainsi, il faut protéger un secret (la clé) qui permet de protéger un autre secret (l'information qui a été chiffrée pour être confidentielle).

Clé privée (*private key*)

Clé utilisée dans les mécanismes de chiffrement asymétrique (ou chiffrement à clé publique) qui appartient à une entité et qui doit être secrète.

Clé publique (*public key*)

De manière générale, en cryptographie asymétrique, la clé publique d'une entité doit être rendue publique aux interlocuteurs qui souhaitent lui envoyer des données chiffrées afin qu'elle puisse les déchiffrer avec sa clé privée correspondante.

Clef de session (*Session key*)

Clé secrète générée *via* un système de chiffrement asymétrique, par les correspondants lors de l'établissement d'une session de travail, dont la durée de vie est limitée à cette session, servant à chiffrer des gros volumes d'informations avec un algorithme de chiffrement symétrique.

Code (*cipher*)

Algorithme de chiffrement qui permet de transformer un texte clair en un texte chiffré.

Condensat, résumé, digest (*digest*)

Résultat sous forme de chaîne de caractères, de l'application d'une fonction de hachage sur une suite d'information.

Confiance (*trust*)

Assurance de celui qui se fie à quelqu'un, à quelque chose (critère qualitatif, suggestif, très relatif).

Confidentialité (*confidentiality*)

Maintien du secret des informations et des transactions. Caractère de ce qui est secret. Objectif de sécurité à réaliser afin de prévenir la divulgation non autorisée d'informations à des tiers qui doit permettre leur protection contre des lectures, écoutes, copies illicites d'origines intentionnelle ou accidentelle durant leur stockage, traitement et transfert (notion de **confidentialité de données** (*data confidentiality*)).

Conformité (*compliance*)

Caractère de ce qui est conforme, qui est en concordance, qui ressemble à..., conformité à certaines normes.

Contre-mesure (*counter measure*)

Fonction, mesure, procédure ou mécanisme dédié à la sécurité d'un système afin d'en réduire le niveau de vulnérabilité et de contrer une menace avant qu'elle ne se réalise en action malveillante.

Contrôle d'accès (*access control*)

Mécanisme permettant de prévenir de l'utilisation non appropriée ou non autorisée d'une ressource (services, systèmes, données, programmes).

Cookies

Fichiers envoyés sur le poste de travail des internautes à leur insu, lors de l'accès à certains sites web, qui récoltent des informations les concernant pour en principe, la personnalisation des services web offerts.

Correctif de sécurité (*patch*)

Rustine de sécurité d'un logiciel pour en supprimer une vulnérabilité qui a été identifiée après son installation.

Cryptanalyse (*cryptanalysis*)

La cryptanalyse comprend l'ensemble des moyens qui permet d'analyser une information préalablement chiffrée, afin de la déchiffrer. Plus un système de chiffrement est robuste, plus sa cryptanalyse est difficile.

Cryptogramme (*cryptogram, cyphertext*)

Données ayant subi une transformation cryptographique, données chiffrées, texte ou message chiffré. Données obtenues par chiffrement.

Cryptographie (*cryptography*)

Application des mathématiques permettant d'écrire de l'information de manière à la rendre inintelligible à ceux ne possédant pas les capacités de la déchiffrer. Voir *Chiffrement*.

Cryptographie à clé publique (*public key cryptography*)

Système de chiffrement asymétrique qui utilise un couple de clés appelé *bi-clé*, composée d'une clé privée secrète et d'une clé publique, publiable. Ces deux clés sont complémentaires et indissociables. La relation mathématique qui les relie ne permet pas de retrouver la clé secrète à partir de la clé publique.

Cryptopériode (*cryptographic period*)

Période de temps pendant laquelle les clés d'un système restent inchangées.

DDoS (*Distributed Denial of Service*)

Attaque par saturation (ou déni de service) lancée simultanément à partir de plusieurs systèmes.

Déni de service (DoS, *Denial of Service*)

Attaque par saturation d'une entité afin qu'elle s'effondre et ne puisse plus réaliser les services attendus d'elle.

Disponibilité (*availability*)

Critère de sécurité permettant que les ressources soient accessibles et utilisables selon les besoins (pas de refus d'accès autorisé aux systèmes, services, données, infrastructures, etc.).

Dissuasion (*dissuasion*)

Mesure destinée à persuader par intimidation, un malveillant à renoncer à effectuer une attaque ou en le persuadant que la valeur de l'enjeu qu'il convoite est inférieure à celle des dommages que le système menacé pourrait lui infliger.

Efficacité (*efficiency*)

Caractère de ce qui produit l'effet attendu, des résultats utiles. Propriété des mesures de sécurité qui assure leur pertinence et leur capacité à réellement bien protéger une ressource.

Empreinte numérique (*digest*) – Voir *Condensat*

Ethique (*ethics*)

Qui concerne les principes de la morale. Ensemble de règles morales adoptées par une communauté.

Fiabilité (*reliabiliy*)

Aptitude d'un système à fonctionner sans incident pendant un temps donné.

Flaming

Technique qui consiste, pour affecter la crédibilité d'un groupe de discussions, à y envoyer un grand nombre de messages peu pertinents.

Flooding

Type de moyen d'intrusion dans des systèmes et qui est basé sur le cassage de mots de passe des utilisateurs.

Floudeur (*flooder*)

Programme malveillant servant à ralentir les communications entre un fournisseur d'accès et un internaute ou à déconnecter ce dernier.

Fonction de hachage (*hash function*)

Dans le contexte du chiffrement, cette fonction est qualifiée également de fonction *digest*. Elle permet de générer, à partir de données qui lui sont fournies en entrée, leur résumé (sorte d'empreinte numérique (*digest*)), plus court que le message original et incompréhensible. Ce résumé peut être ensuite chiffré avec la clé privée de l'émetteur et associée au message à transmettre. Sur réception du message et de son empreinte, le destinataire déchiffre cette dernière avec la clé publique de l'émetteur puis, recalcule à partir du message reçu avec la même fonction *hash*, l'empreinte et la compare ensuite avec celle reçue. Si le résultat est identique, le destinataire a ainsi vérifié l'identité de l'émetteur et est assuré de l'intégrité du message. En effet, si le message est altéré, même légèrement, son empreinte est alors considérablement modifiée.

Fonction de hachage à sens unique (*one-way hash function*)

Fonction permettant de calculer l'empreinte de données, mais pas d'engendrer des données qui ont une empreinte particulière. Cette fonction ne doit pas produire des collisions, c'est-à-dire qu'une même empreinte puisse être générée à partir de différents messages.

Gravité de l'impact (*impact gravity*)

Appréciation du niveau de gravité d'un incident, pondéré par sa fréquence d'apparition. Il est important de pouvoir quantifier ce critère d'impact afin d'identifier au mieux les impératifs de sécurité et les degrés d'urgence de la prise en considération de ces impératifs (exemple de quantification: impact de gravité insignifiante: (0) sans gravité, (1) peu grave, (3) très grave, (4) extrêmement grave).

Hacker, hackeur (*hacker*)

Action consistant à s'introduire de manière illicite dans un système. Personne qui quelle que soit sa motivation, pénètre sans autorisation et de manière illégale, dans un système appartenant à un tiers.

Hacking

Ensemble des opérations permettant une intrusion dans un système informatique

Identification (*identification*)

Processus qui permet de reconnaître une entité préalablement identifiée.

Identité (*identity*)

Information qui permet de désigner et de distinguer, si possible de manière unique et non ambiguë, une entité à l'intérieur d'un domaine de nommage.

Impact (*impact*)

Exprime le niveau des conséquences produites par une atteinte (impact financier, *financial impact*), coût de l'atteinte; **impact logique** (*logical impact*) atteinte aux critères de disponibilité, d'intégrité, de confidentialité, **impact stratégique** (*strategical impact*) préjudiciable à la survie d'une organisation; **impact tangible** (*tangible impact*) atteinte que l'on peut directement constater, réel.

Imputabilité (*imputability*)

Propriété qui permet d'imputer de façon certaine une opération à un utilisateur à un moment donné. Fait de pouvoir identifier un responsable en cas de violation du règlement.

Infrastructure de gestion clés (IGC ou PKI, *Public Key Infrastructure*)

Infrastructure de support à la réalisation de la mise en œuvre du chiffrement asymétrique (à clé publique) offrant entre autres des services de gestion et de distribution de clés de chiffrement et de certificats numériques.

Infrastructure de management des privilèges (PMI, *Privilege Management infrastructure*)

Infrastructure capable de supporter la gestion des privilèges, permissions ou habilitations.

Ingénierie sociale (*social engeneering*)

Techniques, procédures et moyens utilisés par des malveillants profitant le plus souvent de la crédulité des utilisateurs, pour entre autres, soutirer leurs mots de passe et leurs paramètres de connexion, usurper leur identité numérique, afin de leurrer les systèmes et les pénétrer en se faisant passer pour les personnes habilitées.

Innocuité (*safety*)

Qualité de ce qui n'est pas nuisible.

Intégrité (*integrity*)

Etat d'une chose qui est demeurée intacte. Critère de sécurité, qui s'il est réalisé, permet de s'assurer qu'une ressource n'a pas été altérée (modifiée ou détruite) d'une façon non autorisée.

Intranet (*Intranet*)

Réseau interne, réseau privé à une organisation, utilisant les technologies de l'internet et généralement isolé de l'internet par des systèmes *firewall*.

IPSec (*Internet Protocol Security*)

Version du protocole IP qui offre des services de sécurité. IPSec permet de créer un canal logique de communication (tunnel IP), au travers de l'internet public, entre deux correspondants. Les extrémités du tunnel sont authentifiées et les données qui y transitent peuvent être chiffrées (notion de canal chiffré ou de réseau virtuel).

IPv6 (*Internet Protocole version 6*)

Evolution de la version 4 du protocole IP, qui entre autres, intègre en mode natif des mécanismes permettant de réaliser des services de sécurité (authentification des entités source et destination, confidentialité des données transmises).

Logiciel espion *(spyware)*

Programme qui envoie à un malveillant des informations sensibles depuis l'ordinateur compromis.

Logiciel malveillant *(malware)*

Terme générique désignant un programme de type virus, ver, cheval de Troie, etc. ou toute autre forme de logiciel d'attaque qui agit de manière plus ou moins autonome.

Malveillance (*maleovolence*)

Actions à caractère hostile pouvant porter atteinte aux ressources d'une organisation qui peuvent être commises directement ou indirectement par des personnes internes ou externes à celle-ci (vol de matériels, de données, divulgation d'informations confidentielles, intrusions illicites, etc.).

Management des clés (*key management*)

Gestion des clés de chiffrement, génération, distribution, archivage, destructions des clés en fonction de la politique de sécurité.

Management du risque, gestion des risques (*risk management*)

Processus continu d'évaluation des risques encourus par une organisation afin de les maîtriser, de les réduire à un niveau acceptable. Permet de déterminer la politique de sécurité la plus adaptée à la protection des valeurs de l'organisation.

Mascarade (*masquerade*)

Type d'attaque basée sur le leurre des systèmes.

Menace (*threat*)

Signe, indice qui laisse prévoir un danger. Action ou événement susceptible de se produire, de se transformer en agression contre un environnement ou des ressources et de porter préjudice à leur sécurité.

Mesures de sécurité (*security measures*)

Ensemble de moyens technologiques, organisationnels, juridiques, financiers, humains, procéduraux et d'actions permettant d'atteindre les objectifs de sécurité fixés par le politique de sécurité. Les mesures sont généralement classifiées selon leur rôle fonctionnel (ex.: mesure de prévention, de protection, de dissuasion, etc.).

Mot de passe (*password*)

Information confidentielle que doit produire un ayant droit afin de prouver son identité lors d'une procédure d'authentification dans le cadre d'une demande d'accès à une ressource.

Non-répudiation (*non-repudiation*)

La capacité de prévenir le fait qu'un expéditeur démente plus tard avoir envoyé un message ou effectué une action. Assure la disponibilité de preuves qui peuvent être présentées à un tiers et utilisées pour prouver que tel type d'événement ou d'action a eu lieu. Preuve qu'un message a été envoyé par une personne précise à un moment précis, sans avoir été modifié depuis son envoi. Cette preuve devrait pouvoir être vérifiée à tout moment par un tiers. Sans la non-répudiation, des émetteurs et des récepteurs d'informations pourraient nier les avoir reçues ou envoyées.

No-opt

Service dans lequel les clients n'ont pas le choix sur la façon dont les informations les concernant sont utilisées (possibilité d'atteinte à la protection des données privées).

Notarisation (*notarization*)

Enregistrement de données à des fins de preuve.

Panne (*failure*)

Dysfonctionnement, arrêt de fonctionnement entraînant l'indisponibilité d'une ressource.

Pare-feu (*firewall*)

Matériel ou logiciel permettant de réaliser l'isolement, le masquage des ressources, le filtrage des données, le contrôle des flux, contribuant à la protection des environnements informatiques privés d'une organisation connectés à l'internet.

Perte de service essentiel (*lost of essential services*)

Indisponibilité ou dysfonctionnement total ou partiel de ressources nécessaires au bon fonctionnement d'un système, d'une organisation.

Pertes directes (*direct losses*)

Pertes identifiables directement consécutives à un défaut de sécurité.

Pertes indirectes (*indirect losses*)

Pertes générées indirectement par un défaut de sécurité.

Phreak

Utilisation illégale ou détournement, aux dépens d'un individu ou d'un opérateur, des services de télécommunication, par un *phreaker* (notion de *phreaking*).

Pirate, malveillant, attaquant (*hacker*)

Personne qui s'introduit illégalement dans des systèmes afin de réaliser des attaques passives ou actives.

Plan de gestion de crise (*emergency plan*)

Ensemble des moyens techniques et organisationnels prévus pour répondre optimalement à un incident grave affectant la bonne marche des opérations et préjudiciable à l'organisation.

Plan de secours (*backup plan*)

Ensemble des moyens techniques et organisationnels prévus pour assurer la pérennité des informations et la continuité des activités quels que soient les problèmes rencontrés.

Politique de sécurité (*security policy*)

Référentiel de sécurité établi par une organisation, reflétant sa stratégie de sécurité et spécifiant les moyens de la réaliser.

Porte dérobée (*backdoor, trap door*)

Fait le plus souvent référence à un morceau de code intégré dans des logiciels permettant à des entités non autorisées, la prise de contrôle des systèmes, la copie d'information, etc. à l'insu de leur propriétaire.

Prévention (*prevention*)

Ensemble de mesures prises pour prévenir d'un danger, d'un risque, qui tend à empêcher la réalisation de menaces, à réduire la fréquence des incidents dans une optique de protection.

Profil d'utilisateur (*user profile*)

Liste des attributs concernant un utilisateur contribuant à effectuer la gestion du réseau et des systèmes auquel il se connecte (paramètres d'identification, d'authentification, droits d'accès, permissions et toutes autres informations utiles, à des fins de contrôle d'accès, de facturation, etc.).

Protection (*protection*)

Action, fait de protéger. Se dit d'une mesure de sécurité qui contribue à détecter, à neutraliser ou à diminuer les effets d'une agression.

Protection des données privées et de l'intimité numérique (*privacy protection*)

Mesures de protection qui permettent d'assurer que les informations, les activités des internautes, ne soient pas révélées à d'autres parties que celles voulues et ne soient pas utilisées à des fins contraires à celles consenties par leur propriétaire. Cela fait référence au droit des individus de contrôler les informations les concernant qui peuvent être collectées soit directement, soit indirectement par observation de leur comportement de navigation et sites visités.

Répudiation (*repudiation*)

Fait de nier d'avoir participé à des échanges, totalement ou en partie.

Réseau privé virtuel (RPV ou VPN, *Virtual Private Network*)

La notion de réseau privé virtuel fait référence à l'usage du protocole IPSec afin de créer un canal de communication sécurisé à usage privé, au travers d'un réseau public non sécurisé. Souvent mis en œuvre par une organisation, pour connecter ses différents sites *via* l'internet afin d'assurer la confidentialité des données échangées.

Révocation (*revocation*)

Annonce qu'une clé privée a perdu son intégrité. Le certificat de la clé publique correspondante ne doit plus être utilisé.

Risque (*risk*)

Danger plus ou moins probable émanant d'une menace et pouvant se traduire en terme de probabilité d'apparition et de niveau d'impact.

RSSI (Responsable de la Sécurité du Système d'Information)

Personne chargée de la sécurité se rapportant aux systèmes d'information.

Sabotage

Action malveillante, vandalisme, détérioration intentionnée tendant à empêcher le fonctionnement normal d'une organisation, d'une infrastructure, d'un service, d'une ressource pouvant conduire à un sinistre.

Sécurité (*security*)

Situation dans laquelle quelqu'un, quelque chose n'est exposé à aucun danger. Mécanisme destiné à prévenir un événement dommageable, ou à en limiter les effets. Ainsi par exemple, la **sécurité physique** (*physical security*) est relative aux mesures permettant d'offrir une protection physique, matérielle des environnements, tandis que la **sécurité logique** (*logical security*) fait référence aux procédures et moyens logiciels de protection.

Sensibilité (*sensitivity*)

Caractéristique d'une entité qui indique sa valeur ou son importance.

S-http

Version sécurisée du protocole http permettant la sécurité des échanges entre un client et un serveur web.

Signature numérique (*digital signature*)

Par analogie à la signature manuelle, la signature numérique obtenue par un algorithme de chiffrement asymétrique permet d'authentifier l'émetteur d'un message et d'en vérifier l'intégrité.

Sniffer

Logiciel destiné à réaliser des écoutes passives des données transitant dans un réseau.

Sniffing

Action consistant à réaliser des écoutes passives afin de récupérer des paramètres de connexion qui seront par la suite utilisées à l'insu de leurs propriétaires légitimes afin de commettre des intrusions non autorisées.

Spammer

Personne qui réalise le *spamming.*

Spamming

Technique qui consiste à envoyer des messages non désirés sur une messagerie électronique.

Spoofer

Personne qui pratique le spoofing.

Spoofing

Usurpation d'adresses IP à des fins d'intrusion.

SSL (*Secure Sockets Layer*)

Logiciel assurant la sécurité des échanges sur l'internet, développé par Netscape et supporté par la majorité des navigateurs web du marché.

Stéganographie (*Steganography*)

Technique permettant de dissimuler une information dans une autre afin de la transmettre ou de la stocker clandestinement. Le marquage de document, le tatouage *(watermarking),* est une application de la stéganographie qui consiste à marquer une image de façon indélébile.

Système de détection d'intrusion (IDS, *Intrusion Detection System*)

Système permettant de détecter des incidents qui pourraient conduire à des violations de la politique de sécurité et permettant de diagnostiquer des intrusions potentielles.

Test de pénétration (*penetration test*)

Tests pratiqués pour analyser et tester le degré de protection des systèmes et la robustesse des mécanismes de sécurité.

Virus (*virus*)

Programme malveillant introduit, à l'insu des utilisateurs, dans un système. Il possède la capacité de se dupliquer (soit à l'identique, soit en se modifiant (virus polymorphe)), de porter atteinte aux environnements dans lequel il s'exécute, et de contaminer les autres utilisateurs avec lesquels il est en relation. Différents types de virus sont distingués en fonction de leur signature, de leur comportement, de leur type de reproduction, de l'infection, des dysfonctionnements induits, etc. Les **vers**, **chevaux de Troie**, **bombes logiques** sont des codes malveillants de la famille générique des virus.

Vulnérabilité (*vulnerability*)

Défaut de sécurité qui pourrait se traduire soit intentionnellement soit accidentellement par une violation de la politique de sécurité.

Annexe B – Chapitres de la norme ISO/IEC 17799:2005 qui constitue un document de référence en matière de gestion de la sécurité

Introduction
- 0.1 Qu'est-ce que la sécurité de l'information?
- 0.2 Pourquoi la sécurité de l'information est-elle nécessaire?
- 0.3 Comment établir les besoins de sécurité
- 0.4 Evaluer les risques de sécurité
- 0.5 Sélectionner les contrôles
- 0.6 Point de départ en sécurité de l'information
- 0.7 Facteurs de succès critiques X
- 0.8 Développer vos propres directives

1 Portée

2 Terminologie et définitions

3 Structure de la présente norme.
- 3.1 Clauses
- 3.2 Principales catégories de sécurité

4 Evaluation des risques et traitements
- 4.1 Evaluation des risques de sécurité
- 4.2 Traitement des risques de sécurité

5 Politique de sécurité
- 5.1 Politique de sécurité de l'information
  - 5.1.1 Document de politique de sécurité de l'information
  - 5.1.2 Examen de la politique de sécurité de l'information

6 Organisation de la sécurité de l'information
- 6.1 Organisation interne
  - 6.1.1 Engagement de la direction dans la sécurité de l'information.
  - 6.1.2 Coordination de la sécurité de l'information
  - 6.1.3 Attribution des responsabilités pour la sécurité de l'information
  - 6.1.4 Processus d'autorisations pour les équipements de traitement de l'information
  - 6.1.5 Accords de confidentialité
  - 6.1.6 Contact avec les autorités
  - 6.1.7 Contact avec des groupements d'intérêt spécifique
  - 6.1.8 Examen indépendant de la sécurité de l'information
- 6.2 Parties externes
  - 6.2.1 Identification des risques liés aux parties externes
  - 6.2.2 La sécurité en ayant affaire avec des clients
  - 6.2.3 La sécurité dans les accords avec des tiers

7 Gestion des biens et des valeurs
- 7.1 Responsabilités des valeurs
  - 7.1.1 Inventaire des valeurs
  - 7.1.2 Propriété des valeurs
  - 7.1.3 Utilisation acceptable des valeurs
- 7.2 Classification de l'information
  - 7.2.1 Directives de classification
  - 7.2.2 Marquage (étiquetage) et manipulation de l'information

8 Sécurité des ressources humaines
- 8.1 Avant l'emploi
  - 8.1.1 Rôles et responsabilités
  - 8.1.2 Annalyse
  - 8.1.3 Modalités et conditions d'embauche
- 8.2 Durant l'emploi
  - 8.2.1 Responsabilités de la direction
  - 8.2.2 Prise de conscience, sensibilisation, éducation, et formation à la sécurité de l'information
  - 8.2.3 Mesures disciplinaires
- 8.3 Arrêt ou changement d'emploi
  - 8.3.1 Responsabilités de l'arrêt
  - 8.3.2 Restitution des valeurs
  - 8.3.3 Elimination des droits d'accès

9 Sécurité physique et environnementale
- 9.1 Zones de sécurité
  - 9.1.1 Périmètre de sécurité
  - 9.1.2 Contrôles d'accès physique
  - 9.1.3 Sécuriser les bureaux, les salles et les équipements
  - 9.1.4 Protection contre les menaces externes et environnementales
  - 9.1.5 Travailler dans des zones sécurisées
  - 9.1.6 Secteurs d'accès public de livraison et de chargement
- 9.2 Sécurité des équipements
  - 9.2.1 Situation et protection des équipements
  - 9.2.2 Support des utilités
  - 9.2.3 Sécurité du câblage
  - 9.2.4 Maintenance des équipements
  - 9.2.5 Sécurité des équipements en dehors des frontières de l'organisation
  - 9.2.6 Sécurité des équipements abandonnés ou réutilisés
  - 9.2.7 Suppression des équipements

10 Gestion des communications et des opérations
- 10.1 Procédures opérationnelles et responsabilités
  - 10.1.1 Modes opératoires documentés
  - 10.1.2 Gestion du changement
  - 10.1.3 Ségrégation des fonctions
  - 10.1.4 Séparation des facilités liées au développement, aux tests et aux opérations
- 10.2 Gestion de la livraison de services offerts par des tiers
  - 10.2.1 Livraison de services
  - 10.2.2 Surveillance et contrôle des services fournis par des tiers
  - 10.2.3 Gestion des changements dans les services offerts par des tiers
- 10.3 Planification et acceptation de systèmes
  - 10.3.1 Gestion de la capacité
  - 10.3.2 Tolérance des systèmes
- 10.4 Protection contre les codes malicieux et mobiles
  - 10.4.1 Contrôles contre le code malicieux
  - 10.4.2 Contrôles contre les codes mobiles

- 10.5 Back-up /secours
  - 10.5.1 Back-up des informations
- 10.6 Gestion de la sécurité des réseaux
  - 10.6.1 Contrôle du réseau
  - 10.6.2 Sécurité des services réseau
- 10.7 Manipulation de supports
  - 10.7.1 Gestion des supports amovibles
  - 10.7.2 Destruction des supports
  - 10.7.3 Procédures de manipulation de données
  - 10.7.4 Sécurité de la documentation des systèmes
- 10.8 Echange d'informations
  - 10.8.1 Politiques et procédures d'échange d'information
  - 10.8.2 Accords d'échange
  - 10.8.3 Supports physiques en transit
  - 10.8.4 Messagerie électronique
  - 10.8.5 Systèmes d'information
- 10.9 Services de commerce électronique
  - 10.9.1 Commerce électronique
  - 10.9.2 Transactions en ligne
  - 10.9.3 Information accessible au public
- 10.10 Surveillance
  - 10.10.1 Audit des journaux (*logs*)
  - 10.10.2 Surveillance de l'utilisation du système
  - 10.10.3 Protection des informations journalisées
  - 10.10.4 Journaux des administrateurs et opérateurs
  - 10.10.5 Journalisation des erreurs et incidents
  - 10.10.6 Synchronisation des horloges

11 Contrôles d'accès

- 11.1 Impératifs de l'organisation (besoins du business) en matière de contrôle d'accès
  - 11.1.1 Politique de contrôle d'accès
- 11.2 Gestion des accès des utilisateurs
  - 11.2.1 Enregistrement des utilisateurs
  - 11.2.2 Gestion des privilèges
  - 11.2.3 Gestion des mots de passe des utilisateurs
  - 11.2.4 Examen des droits d'accès des utilisateurs
- 11.3 Responsabilités des utilisateurs
  - 11.3.1 Utilisation des mots de passé
  - 11.3.2 Equipements des utilisateurs sans surveillance
  - 11.3.3 Politique concernant les bureaux et écrans clairs
- 11.4 Contrôle de l'accès au réseau
  - 11.4.1 Politique sur l'utilisation des services de réseau
  - 11.4.2 Authentification des utilisateurs pour les connexions externes
  - 11.4.3 Identification des équipements dans les réseaux
  - 11.4.4 Protection des ports de télédiagnostique et de téléconfiguration
  - 11.4.5 Ségrégation dans les réseaux
  - 11.4.6 Contrôle de la connexion réseau
  - 11.4.7 Contrôle du routage réseaux

- 11.5 Contrôle d'accès aux système d'exploitation
  - 11.5.1 Procédures de connexion sécurisées
  - 11.5.2 Identification et authentification des utilisateurs
  - 11.5.3 Système de gestion des mots de passe
  - 11.5.4 Utilisation des utilitaires système
  - 11.5.5 Délai de session (*time-out*)
  - 11.5.6 Limitation du temps de connexion
- 11.6 Contrôle d'accès aux applications et aux informations
  - 11.6.1 Restriction de l'accès aux informations
  - 11.6.2 Isolation des systèmes sensibles
- 11.7 Mobilité en informatique et télétravail
  - 11.7.1 Mobilité et communications
  - 11.7.2 Télétravail

12 Acquisition, développement et maintenance des systèmes d'information
- 12.1 Besoins de sécurité pour les systèmes d'information
  - 12.1.1 Analyse et spécification des besoins de sécurité
- 12.2 Exactitude des traitements applicatifs
  - 12.2.1 Validation des données saisies
  - 12.2.2 Contrôle du traitement interne
  - 12.2.3 Intégrité des messages
  - 12.2.4 Validation des résultats
- 12.3 Controles du chiffrement
  - 12.3.1 Politique de contrôle de l'usage de la cryptographie
  - 12.3.2 Gestion des clés
- 12.4 Sécurité des fichiers systèmes
  - 12.4.1 Contrôle des logiciels opérationnels
  - 12.4.2 Protection des données de tests du système
  - 12.4.3 Contrôle d'accès au code source des programmes
- 12.5 Sécurité dans le développement et le support des processus
  - 12.5.1 Procédures de contrôle du changement
  - 12.5.2 Examen technique des applications après modification du système d'exploitation
  - 12.5.3 Restrictions des changements dans les suites logicielles
  - 12.5.4 Fuite d'information
  - 12.5.5 Développement externalisé des de logiciels
- 12.6 Gestion des vulnérabilités techniques
  - 12.6.1 Contrôle des vulnérabilités techniques

13 Gestion des incidents de sécurité de l'information
- 13.1 Notification des évènements et des faiblesses de sécurité de l'information
  - 13.1.1 Notification des événements de sécurité de l'information
  - 13.1.2 Notification des faiblesses de sécurité
- 13.2 Gestion des incidents et des améliorations de la sécurité de l'information
  - 13.2.1 Responsabilités et procédures
  - 13.2.2 Enseignement à tirer des incidents de sécurité
  - 13.2.3 Collecte de preuves

14 Gestion de la continuité des affaires
- 14.1 Aspects sécuritaires de la gestion de la continuité des affaires
  - 14.1.1 Inclure la sécurité de l'information dans le processus de gestion de la continuité des affaires
  - 14.1.2 Continuité des affaires et évaluation des risques
  - 14.1.3 Développer et implementer des plans de continuité intégrant la sécurité de l'information
  - 14.1.4 Cadre de planification de la continuité des activités
  - 14.1.5 Test, maintenance et ré-évaluation des plans de continuité

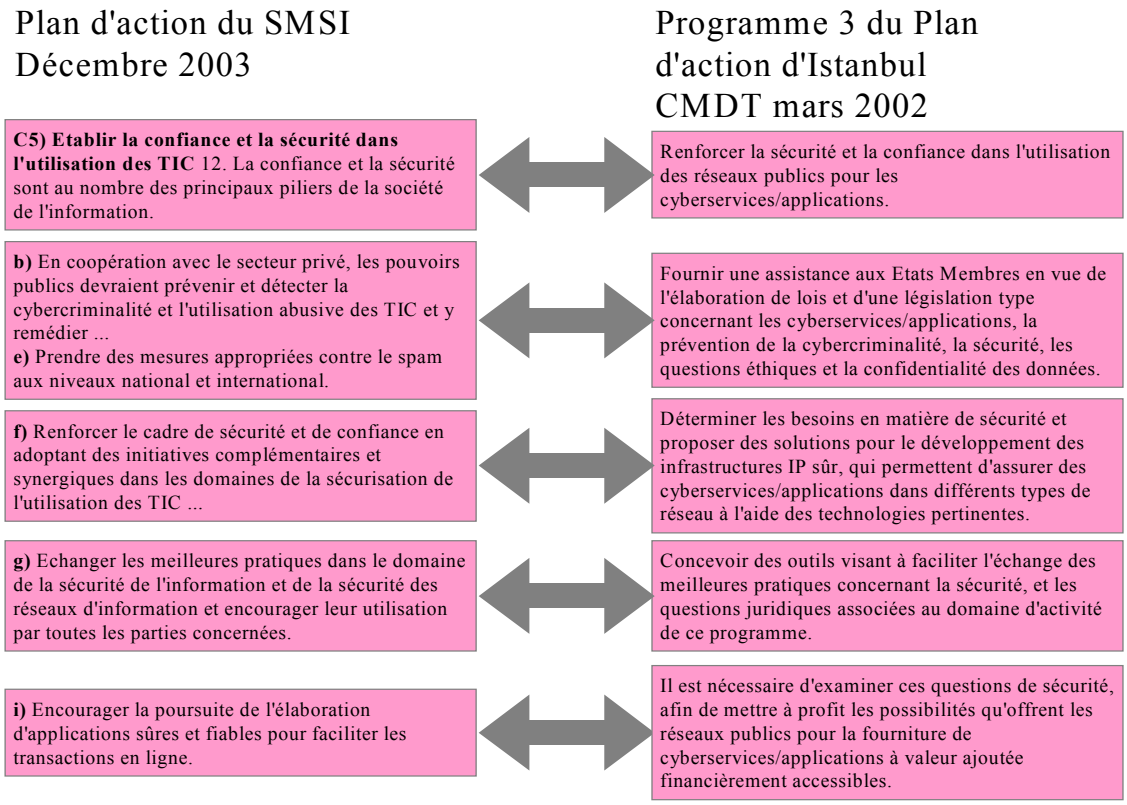
15 Conformité
- 15.1 Conformité aux exigences légales
  - 15.1.1 Identification de la législation applicable
  - 15.1.2 Droits de la propriété intellectuelle
  - 15.1.3 Protection des enregistrements de l'organisation
  - 15.1.4 Protection des données et intimité numérique
  - 15.1.5 Prévention du détournement des facilités de traitement de l'information
  - 15.1.6 Réglementation des contrôles de cryptographie
- 15.2 Conformité avec les normes et politiques de sécurité et conformité technique
  - 15.2.1 Conformité avec les politiques et les de sécurité
  - 15.2.2 Contrôle de la conformité technique
- 15.3 Considérations sur l'audit des systèmes d'information
  - 15.3.1 Contrôle des audits des systèmes d'information
  - 15.3.2 Protection des outils d'audit des systèmes d'information

Bibliographie et Index

Annexe C – Mandat et activités de l'UIT-D dans le domaine de la cybersécurité

Pour tout complément d'information, veuillez consulter le site:
http://www.itu.int/ITU-D/e-strategy/e-security

La correspondance quasi parfaite entre les priorités du Programme sur la cybersécurité et le Plan d'action du SMSI (Genève) illustre la forte synergie entre ces deux documents. Conformément à l'Agenda de Tunis de 2005, l'UIT a été désignée coordonnateur et modérateur pour les initiatives liées à la mise en oeuvre du Plan d'action de Genève en ce qui concerne l'établissement de la confiance et de la sécurité dans l'utilisation des TIC. A l'UIT-D, la cybersécurité pour les applications TIC est l'un des six domaines prioritaires du Programme 3 du Plan d'action d'Istanbul.



Activités de l'UIT-D dans le domaine de la sécurité et de la confiance

Dans le cadre du Programme 3 du Plan d'action d'Istanbul de la CMDT-02, l'UIT aide les pays en développement à mettre en oeuvre leurs projets, leur donne des avis pour l'élaboration de leurs politiques et de leurs stratégies, ainsi que d'une législation appropriée encourageant le développement et l'utilisation de la cybersécurité et de la confiance pour la réalisation de transactions critiques dans des domaines comme la santé, l'éducation et le commerce et les communications entre administrations et fonctionnaires publics.

Projets visant à offrir des services garantissant sécurité et confiance pour les applications TIC

Des projets utilisant des technologies évoluées garantissant sécurité et confiance, basées sur une infrastructure à clés publiques (PKI) (techniques de l'authentification biométrique, des cartes intelligentes, des certificats numériques et des signatures numériques UIT-T X.509) ont été mis en oeuvre et sont opérationnels en Bulgarie, au Burkina Faso, en Côte d'Ivoire, au Cambodge, en Géorgie, au Pérou, au Sénégal, au Paraguay et en Turquie (secteur privé). Pour la période 2004-2005, des activités sur les techniques de cybersécurité et les applications TIC sont actuellement en cours ou ont été menées à bien en Afghanistan, en Barbade, au Bhoutan, en Bulgarie (Phase III), au Cameroun, en Jamaïque, au Rwanda, en Turquie (télésanté et administration publique en ligne) et en Zambie (signatures électroniques).

Grâce à l'UIT, plusieurs pays en développement ont, pour la première fois, participé activement à la mise en place et à l'utilisation de services visant à établir la confiance et la sécurité. Ainsi les TIC ont des retombées bénéfiques non seulement dans le secteur du commerce mais aussi au niveau de la société tout entière, qu'il s'agisse de l'administration publique ou de la santé.

Des projets utilisant des technologies évoluées de sécurité et de confiance, basées sur une infrastructure à clés publiques (PKI) (techniques de l'authentification biométrique, des cartes intelligentes, des certificats numériques et des signatures numériques UIT-T X.509), ont été mis en oeuvre ou sont en cours de mise en oeuvre en Barbade, au Bhoutan, en Bulgarie, au Burkina Faso, au Cambodge, au Cameroun, en Côte d'Ivoire, en Géorgie, en Jamaïque, au Pérou, au Sénégal, au Paraguay, en Turquie et en Zambie.

En Géorgie, l'UIT propose des solutions rentables pour sécuriser la transmission et le traitement des documents numérisés des administrations publiques et l'accès à ces documents, ce qui permettra d'améliorer l'efficacité et la transparence des services publics. Les fonctionnaires de haut niveau du Ministère des transports et des communications de la Géorgie bénéficieront en effet de systèmes permettant d'automatiser les flux de travail, de signer et de diffuser numériquement les documents officiels, remplaçant les méthodes "papier" lentes et assez coûteuses. Il sera possible d'obtenir un accès autorisé à des documents sensibles grâce à des systèmes de sécurité et de confiance qui permettront d'établir l'identité des fonctionnaires autorisés au sein du Ministère.

Au Paraguay, l'UIT a fourni une assistance pour la mise en oeuvre d'une plate-forme fournissant un mécanisme internet de sécurité et de confiance que les opérateurs et les fournisseurs de services pourront utiliser pour échanger des informations sensibles (par exemple les déclarations de revenus) en format électronique avec l'Autorité nationale de réglementation. Les outils TIC sont utilisés pour rationaliser le processus d'octroi de licences aux opérateurs de téléphonie publics et pour accroître l'efficacité des opérations commerciales du régulateur.

Une assistance a été fournie pour définir le cadre d'une politique nationale sur l'utilisation des certificats numériques et le fonctionnement des autorités de certification. L'UIT a également apporté une assistance pour l'élaboration des spécifications techniques et a fourni des avis de politique générale pour mettre en place en Jamaïque et en Barbade une plate-forme pour la publication et la gestion des certificats numériques, offrant ainsi des services d'authentification robuste et assurant sécurité et confiance pour les transactions en ligne de l'administration publique ou les transactions de commerce électronique.

Au Cameroun, le projet de l'UIT permet de sécuriser la transmission sur l'internet de documents sensibles de l'administration publique et d'offrir des services administratifs en ligne aux citoyens vivant dans des zones urbaines ou isolées où il n'y a aucune infrastructure administrative physique. L'authentification robuste, la confidentialité des données, l'intégrité des données et la non-répudiation de l'information, autant de systèmes basés sur les techniques de cryptage et de signature électronique permettent de régler certains problèmes de sécurité, notamment l'usurpation d'identité.

En Bulgarie, l'assistance fournie par l'UIT pour la mise en oeuvre d'une plate-forme de cybersécurité permet d'assurer des communications extrêmement fiables entre le Ministère des transports et des communications, le Ministère des finances, le Conseil des ministres et la Commission chargée de la réglementation des communications (CRC), en utilisant une infrastructure à clés publiques (PKI) et des applications compatibles PKI. Cette plate-forme permet une interaction sécurisée, efficace et rentable entre les hauts fonctionnaires du gouvernement, en complément des réunions "physiques" et améliore la productivité. Toutes les données échangées entre les fonctionnaires sont sécurisées, signées numériquement grâce à l'utilisation des techniques de confidentialité des données, de non-répudiation de l'information, d'intégrité des données et d'authentification robuste.

L'objectif stratégique du projet est d'améliorer les services de soins de santé en Turquie en mettant en place un support d'information sur la santé sécurisé qui permet aux prestataires de soins de santé (soins de santé primaires et secondaires), aux professionnels de la santé et aux citoyens d'avoir accès facilement et de façon sûre, à des informations dans le domaine de la santé en utilisant les TIC les plus récentes.

Les éléments essentiels de ce programme sont l'élaboration de systèmes d'information pour les soins de santé primaires en complément du réseau des médecins de famille, la mise en place de dossiers médicaux électroniques et le développement de systèmes interopérables entre les fournisseurs de services de soins de santé, notamment les centres de soins de santé primaires, les hôpitaux et les sociétés d'assurance publiques et privées.

Politiques et stratégies nationales et régionales

Un atelier a été organisé à l'intention de 128 pays afin de partager les informations et les meilleures pratiques sur les technologies de sécurité et de confiance et sur les politiques applicables au commerce électronique.

L'UIT a organisé des ateliers et des séminaires sur les stratégies relatives aux techniques de cybersécurité dans un certain nombre de pays (par exemple, Azerbaïdjan, Cameroun, Chili (pour les pays du Mercusor), Mongolie, Pakistan, Paraguay, Roumanie, Seychelles, République arabe syrienne et Ouzbékistan). La sécurité et la confiance ont été parmi les principaux thèmes abordés au Colloque régional organisé par l'UIT en novembre 2004 sur l'administration publique en ligne et le protocole internet à l'intention des Etats de la région arabe. Ce colloque a abouti à la Déclaration de Dubaï, laquelle souligne qu'il est nécessaire que l'UIT poursuive ses activités dans le domaine de la cybersécurité pour les cyberapplications et les cyberservices.

Un manuel sur la cybersécurité est actuellement en cours d'élaboration afin d'aider les pays en développement et les pays les moins avancés à renforcer leurs capacités locales et à mieux connaître certains des problèmes essentiels que pose la sécurité pour la société de l'information. Ce manuel donnera des explications sur certains des grands problèmes comme le spam, les logiciels furtifs néfastes ou malware (virus, vers, chevaux de Troie), le caractère confidentiel des données, l'absence d'authentification, la nécessité de la confidentialité et de l'intégrité des données. D'autres sujets ont été abordés lors de ce colloque, qui devait se terminer en novembre 2005, notamment l'élaboration de lignes directrices et de meilleures pratiques sur une législation relative à la cybersécurité et des exemples de méthodes utilisées pour protéger les infrastructures critiques ont été donnés. En 2005, l'UIT-D a organisé les manifestations suivantes:

1 UIT/Union européenne (ENISA) - Séminaire régional sur la cybersécurité pour la CEE, les pays de la CEI et les Etats baltes.

2 Séminaire sous-régional sur la cybersécurité pour les réseaux d'information et de communication.

3 Réunion thématique du SMSI sur la cybersécurité organisée par l'UIT-D, l'UIT-T et le Secrétariat général.

Assistance fournie pour l'élaboration d'une législation appropriée

L'utilisation des applications TIC suppose l'existence d'un environnement juridique et politique approprié pour régler des questions comme le caractère confidentiel des données, la prévention du cybercrime, la sécurité, les problèmes d'éthique, les signatures électroniques, les autorités de certification et les contrats électroniques pour susciter la confiance, protéger les droits et encourager l'utilisation des applications TIC.

L'UIT a fourni une assistance aux pays suivants pour l'élaboration d'un modèle de législation couvrant des domaines comme le commerce électronique, la protection des données, les transactions en ligne, la certification, l'authentification et le cryptage numériques: les Etats Membres de l'ASETA (Bolivie, Colombie, Equateur, Pérou et Venezuela), le Burkina Faso, le Cap-Vert, la Mauritanie, la Mongolie et la Tanzanie.

Dans le cadre des efforts qu'elle déploie pour fournir aux pays en développement des lignes directrices et des études de cas consacrées à l'élaboration d'une législation sur la confidentialité des données, les applications TIC, la prévention du cybercrime, l'UIT a publié un rapport basé sur des recherches ainsi qu'une analyse contenant des exemples concrets illustrant comment certains pays ont élaboré une législation sur la prévention du cybercrime. Ce travail a été fait par Mme Michela Menting Yoell de l'Université d'Essex (Angleterre) dans le cadre d'un stage de trois mois à l'Unité E-strategies de l'UIT/BDT pour l'obtention de son diplôme LLM en technologies de l'information, média et commerce électronique. Une version PDF de ce rapport peut être téléchargée à l'adresse suivante: Recherche sur la législation relative au caractère confidentiel des données, à la sécurité et à la prévention du cybercrime.

Annexe D – Principales questions en matière de sécurité qui font l'objet de travaux au sein de l'UIT-T durant la période 2005-2008

Issu du site

http://www.itu.int/ITU-T/studygroups/com17/questions.html

Questions attribuées à la Commission d'études 17 de l'UIT-T (période d'études 2005-2008)

Commission d'études 17: Sécurité, langages et logiciels de télécommunication

Question 2/17 – Services d'annuaire, systèmes d'annuaire et certificats d'attributs et de clés publiques

2.1 Services d'annuaire

a) Quelles définitions et quels profils de services nouveaux faut-il adopter pour tirer parti de techniques d'annuaire aussi répandues que X.500 et LDAP, par exemple?

b) Quelles modifications faut-il apporter aux Recommandations des séries E et F et/ou quelles nouvelles Recommandations faut-il élaborer pour spécifier les améliorations à apporter aux définitions et profils de services d'annuaire existants et pour en corriger les défauts?

2.2 Systèmes d'annuaire

a) Quelles améliorations faut-il apporter à l'annuaire afin de l'adapter aux besoins des utilisateurs actuels et potentiels, par exemple obtention d'une meilleure homogénéité des informations d'annuaire dans les sites où elles sont recopiées, opération de prise en charge des informations ajoutées aux attributs d'annuaire par les utilisateurs, amélioration de la qualité de fonctionnement lors de l'extraction d'un nombre élevé de réponses ou solutions proposées pour régler les cas de confusion liée à la détention sous des noms identiques d'informations différentes par plusieurs fournisseurs de services d'annuaire?

b) Quelles autres améliorations faut-il apporter à l'annuaire pour autoriser l'interfonctionnement avec des services mis en oeuvre à l'aide de la spécification LDAP de l'IETF, y compris l'utilisation éventuelle de XML pour l'accès aux annuaires, ainsi que leur prise en charge?

c) Quelles autres améliorations faut-il apporter à l'annuaire et aux certificats d'attributs et de clés publiques pour permettre leur utilisation dans des environnements limités en ressources, par exemple, les réseaux hertziens et les réseaux multimédias?

d) Quelles autres améliorations faut-il apporter à l'annuaire pour en améliorer l'intégration dans des domaines tels que les services de réseau intelligent, de réseaux de télécommunication et d'annuaire publics?

e) Quelles modifications faut-il apporter aux Recommandations de la série X.500 et/ou quelles sont les nouvelles Recommandations à élaborer pour mieux définir les améliorations de l'annuaire et pour trouver des solutions à ses imperfections?

L'étude consacrée aux systèmes d'annuaire sera réalisée en coopération avec le JTC 1 de l'ISO/CEI dans le cadre du travail qu'il consacre à l'extension de la norme ISO/CEI 9594, texte commun aux Recommandations X.500-X.530. Une liaison et une étroite coopération seront en outre maintenues avec l'IETF, en particulier dans les domaines du LDAP.

2.3 Certificats d'attributs et de clés publiques

a) Quelles autres améliorations faut-il apporter aux certificats d'attributs et de clés publiques pour permettre leur utilisation dans des environnements limités en ressources, par exemple, les réseaux hertziens et les réseaux multimédias?

b) Quelles autres améliorations faut-il apporter aux certificats d'attributs et de clés publiques pour accroître leur utilité dans des domaines tels que la biométrie, l'authentification, la commande d'accès et le commerce électronique?

c) Quelles modifications faut-il apporter à la Recommandation X.509 pour mieux définir les améliorations de la Recommandation X.509 et pour trouver des solutions à ses imperfections?

L'étude consacrée aux certificats d'attributs et de clés publiques sera réalisée en coopération avec le JTC 1 de l'ISO/CEI dans le cadre du travail qu'il consacre à l'extension de la norme ISO/CEI 9594-8, texte commun à la Recommandation X.509. Une liaison et une étroite coopération seront en outre maintenues avec l'IETF, en particulier dans les domaines de la PKI.

Question 4/17 – Projet relatif à la sécurité des systèmes de communication (Suite de la Question G/17)

Le domaine de la sécurité est vaste et couvre de nombreux sujets. La sécurité peut être appliquée à la quasi-totalité des aspects des technologies des télécommunications et de l'information. Pour spécifier les exigences de sécurité, il est possible de choisir entre deux méthodes:

– La méthode ascendante, en vertu de laquelle les experts du domaine élaborent des mesures de sécurité visant à renforcer et à protéger le domaine du réseau qui leur incombe, par exemple, biométrie, cryptographie, etc. Cette méthode est la plus répandue mais l'étude de la sécurité, telle qu'elle est effectuée dans les différentes organisations, est fragmentée.

– La méthode descendante offre une vision stratégique et de haut niveau de la sécurité. Dans cette méthode, il est indispensable d'avoir un aperçu général de la situation. Cette méthode est aussi la plus complexe car il est plus difficile de trouver des experts qui possèdent une connaissance détaillée de chaque partie du réseau et de leurs exigences de sécurité, que des experts du sujet qui possèdent, quant à eux, une connaissance spécifique d'un ou deux domaines.

– Une autre solution consiste à combiner les deux méthodes précitées, étant entendu qu'elle suppose une coordination indispensable. Cette façon de procéder a souvent posé de nombreux problèmes, en raison des différents intérêts et programmes dont il faut tenir compte.

La présente Question vise à fixer de grands principes mais aussi à assurer la coordination et l'organisation de toute la gamme des activités à déployer dans le domaine de la sécurité des communications à l'UIT-T. La méthode descendante sera utilisée en collaboration avec d'autres Commissions d'études et d'autres organisations de normalisation. Ce projet vise à mettre en place une méthode plus ciblée au niveau des projets et des stratégies.

Questions

a) Quels sont les résultats attendus du projet relatif à la sécurité des systèmes de communication?

b) Quels sont les processus, sujets d'étude, méthodes de travail et délai à prévoir pour obtenir les résultats attendus dans le cadre du projet?

c) Quels recueils de textes et quels manuels sur la sécurité devront être élaborés et mis à jour par l'UIT?

d) Quels ateliers sur la sécurité faudra-t-il organiser?

e) Quelles mesures faut-il prendre pour nouer des relations efficaces avec d'autres organisations de normalisation en vue de progresser dans le domaine de la sécurité?

f) Quels sont les principales étapes et les critères déterminants du succès?

g) Comment stimuler l'intérêt des Membres du Secteur et des administrations et les encourager à poursuivre les efforts engagés dans le domaine de la sécurité?

h) Comment faire en sorte que les fonctions de sécurité retiennent davantage l'attention du marché?

i) Comment bien faire comprendre aux gouvernements qu'il est indispensable et urgent de protéger les intérêts économiques au niveau mondial, qui dépendent d'une infrastructure robuste et sécurisée des télécommunications?

Question 5/17 - Architecture et cadre général de la sécurité

Compte tenu des dangers qui menacent la sécurité du secteur de la communication et des progrès réalisés dans le domaine des contre-mesures de protection, il convient d'explorer les nouveaux besoins en matière de sécurité ainsi que leurs solutions.

Il convient d'étudier à la fois la sécurité applicable aux nouveaux types de réseaux et la sécurité applicable aux nouveaux services.

2 Questions

a) Comment faut-il définir une solution complète et cohérente en matière de sécurité de communication?

b) Quelle architecture faut-il appliquer pour une solution complète et cohérente en matière de sécurité de communication?

c) Quel est le cadre d'application de l'architecture de sécurité pour élaborer une nouvelle solution de sécurité?

d) Sur quel cadre d'application de l'architecture de sécurité faut-il s'appuyer pour évaluer (et donc améliorer) une solution de sécurité existante?

e) Quelles sont les bases architecturales de la sécurité?

   i) Quelle est l'architecture de sécurité des technologies émergentes?

   ii) Quelle est l'architecture pour la sécurité de bout en bout?

   iii) Quelle est l'architecture de sécurité pour l'environnement mobile?

   iv) Quelles architectures de sécurité technique sont nécessaires? Par exemple:

      a) Quelle est l'architecture de sécurité pour les systèmes ouverts?

      b) Quelle est l'architecture de sécurité pour les réseaux IP?

      c) Quelle est l'architecture de sécurité pour le réseau NGN?

f) Comment convient-il de modifier les Recommandations sur les modèles de sécurité des couches supérieures et inférieures afin de les adapter à l'évolution de l'environnement et quelles nouvelles Recommandations peuvent être nécessaires?

g) Comment faut-il structurer les normes architecturales en ce qui concerne les Recommandations existantes sur la sécurité?

h) Comment convient-il de modifier les Recommandations définissant le cadre de sécurité pour les adapter aux technologies émergentes et quelles nouvelles Recommandations peuvent être nécessaires?

i) Comment interviennent les services de sécurité pour proposer des solutions de sécurité?

Question 6/17 – Cybersécurité

De nombreux mécanismes de protection et de détection ont été mis en oeuvre: pare-feux et systèmes de détection d'intrusion (IDS), mais la plupart d'entre eux privilégient uniquement les aspects techniques. S'il est vrai que ces solutions techniques sont importantes, il est nécessaire d'étudier plus avant la cybersécurité du point de vue de la normalisation sur le plan international.

2 Questions

Il convient d'étudier les domaines ci-après de la cybersécurité:

- processus de distribution, de partage et de divulgation de l'information sur la vulnérabilité;
- procédure normalisée des opérations de traitement des incidents dans le cyberespace;
- stratégie de protection de l'infrastructure critique du réseau.

Question 7/17 - Gestion de la sécurité

2 Questions

a) Comment faut-il définir et gérer les dangers qui menacent les systèmes de télécommunication?

b) Comment faut-il déterminer et gérer les actifs en matière d'information des systèmes de télécommunication?

c) Comment faut-il identifier les questions qui concernent en particulier la gestion des entreprises de télécommunication?

d) Comment faut-il construire correctement des systèmes de gestion de la sécurité de l'information (ISMS) pour les opérateurs de télécommunication, conformément aux normes actuelles en matière d'ISMS?

e) Comment faut-il traiter et gérer les incidents de sécurité dans les télécommunications?

Question 8/17 – Télébiométrie (Suite de la Question K/17)

2 Questions

a) Comment peut-on améliorer l'identification et l'authentification des utilisateurs par l'utilisation de méthodes sécurisées de télébiométrie?

b) Comment la nouvelle partie de la Norme CEI 60027 «Sous-ensemble physiologique» sera-t-elle utilisée à l'UIT-T pour fournir les éléments d'un modèle approprié de classement des dispositifs sécurisés de télébiométrie?

c) Comment utiliser les systèmes de référenciation des niveaux de sécurité pour incorporer les solutions de télébiométrie dans un ordre hiérarchique?

d) Comment faut-il identifier les technologies d'authentifications biométriques pour les télécommunications?

e) Comment faut-il identifier les spécifications des technologies d'authentifications biométriques pour les télécommunications à partir de la technologie de cryptographie comme l'infrastructure PKI?

f) Comment faut-il identifier le modèle et la procédure des technologies d'authentifications biométriques pour les télécommunications à partir de la technologie de cryptographie comme l'infrastructure PKI?

Question 9/17 - Services de communication sécurisés (Suite de la Question L/17)

2 Questions

a) Comment faut-il identifier et définir les services de communication sécurisés dans les services de communications mobiles ou les services du web?

b) Comment faut-il identifier et prendre en charge les menaces qui pèsent sur les services de communication?

c) Quelles sont les technologies de sécurité qui permettent de prendre en charge les services de communication sécurisés?

d) Comment maintenir une interconnectivité sécurisée entre les systèmes de communication?

e) Quelles techniques de sécurité sont nécessaires pour offrir des services de communication sécurisés?

f) Quelles techniques et quels protocoles de sécurité sont nécessaires pour les nouveaux services sécurisés du web?

g) Quels protocoles d'application sécurisés faut-il appliquer aux services de communication sécurisés?

h) Quelles sont les solutions de sécurité globales applicables aux services de communication sécurisés et à leurs applications?

Annexe E – Références bibliographiques

Texte de référence présentant de manière pédagogique les normes de la sécurité du monde des télécommunications élaborées par l'UIT-T:

> *Security in telecommunications and information technology: an overview of issues and the deployment of existing ITU-T Recommendations for secure telecommunication. ITU – T; October 2004 Site web: http://www.itu.int/itudoc/itu-t/86435.html*

Quelques ouvrages de référence

Anderson Ross, Security Engineering, A Guide To Building Dependable Distributed Systems, Wiley, 2001, ISBN 0-471-38922-6

Bishop Matt, Computer security: art and science, Addisson-Wesley, 2002, ISBN 0-201-44099-7

Black Uyless, Internet Security Protocols, Protecting IP Traffic, Pentice Hall, ISBN 0-13-014249-2

Denning Dorothy E., Information Warfare and Security, Addison-Wesley, 1999, ISBN 0-201-43303-6

Dufour Arnaud, Ghernaouti-Hélie Solange; Internet – PUF, Que sais-je? N° 3073 – ISBN: 2-13-053190-3

Ferguson Niels, Schneier Bruce, Practical Cryptography, Wiley, 2003, ISBN 0-471-22357-3

Ghernaouti-Hélie Solange; Internet & Sécurité – PUF Que sais-je? N° 3609 – ISBN: 2-13-051010-8

Ghernaouti-Hélie Solange; Sécurité informatique et réseaux, cours et exercices corrigés – Dunod 2006.

Panko Raymond, Sécurité des systèmes d'information et des réseaux, Pearson Education (version française), 2004

Poulin Guillaume, Soyer Julien, Trioullier Marc-Éric, Sécurité des architectures Web, «ne pas prévoir c'est déjà gémir», Dunod, 2004.

Schneier Bruce, Beyond Fear, Thinking Sensibly About Security In An Uncertain World, Copernicus Books, 2003, ISBN 0-387-02620-7

Schneier Bruce, Secrets et mensonges, la sécurité numérique dans un monde en réseau, Vuibert, (version française) 2001, ISBN 2-711786-846

Schneier Bruce, Cryptographie Appliquée, Algorithmes, protocoles et codes source en C, 2ème édition, Vuibert, 2001, ISBN 2-7117-8676-5 – version française de Schneier Bruce, Applied Cryptography, Protocols, Algorithms and Source Code in C, Second Edition, Wiley, 1996, ISBN 0-471-11709-9

Singh Simon, Histoire des codes secrets, JC Lattès, 1999, ISBN 2-7096-2048-0

Stallings William, Cryptography And Network Security, principles and practice, Prentice Hall, 1999, ISBN 0-13-869017-0

Stallings William, Network And Internetwork Security, principles and practice, Prentice Hall, 1995, ISBN 0-13-180050-7

Stallings William, Network Security Essentials, applications and standards, Prentice Hall, 2000, ISBN 0-13-016093-8

Sites de références

Sites en français:

Site du Premier Ministre (F): http://www.premier-ministre.gouv.fr

Voir particulièrement la rubrique Technologie de l'information dans la thématique: communication.

Site http://www.internet.gouv.fr: site consacré au développement de la société de l'information

Portail de l'administration française: http://www.service-public.gouv.fr. A partir de ce site, on peut retrouver tous les services en ligne, et particulièrement sous la rubrique «se documenter»

Site du service public relatif au droit: http://www.legifrance.gouv.fr

Site de la direction de la documentation française: http://www.ladocfrancaise.gouv.fr

Site http://www.foruminternet.org/: Espace d'information et de débat sur le droit de et sur l'internet et des réseaux

Site de la Commission nationale de l'informatique et des libertés (F): http://www.cnil.fr

Site de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (F): http://www.interieur.gouv.fr/rubriques/c/c3_police_nationale/c3312_oclctic

Observatoire de la sécurité des systèmes d'information et des réseaux: http://www.ossir.org

Site du Clusif: www.clusif.asso.fr. Panorama de la cybercriminalité:

https://www.clusif.asso.fr/fr/production/ouvrages/

Autres sites

Site du CERT: www.cert.org

Site du NIST: http://www.nist.gov; site du National Institute of Standards and Technology (NIST) aux Etats-Unis

Site de la NSA: http://www.nsa.gov; site de la National Security Agency aux Etats-Unis

Site du CSE: http://www.cse.dnd.ca; le Centre de la Sécurité des Télécommunications au Canada

Site du CESG: http://www.cesg.gov.uk; de la National Technical Authority for Information Assurance en Grande-Bretagne

Site du BSI: http://www.bsi.bund.de. Le BSI est l'Office Fédéral de la Sécurité de l'Information en Allemagne. Ce site est en anglais et allemand

Site du DSD: http://www.dsd.gov.au; site du Defence Signals Directorate présente en Australie et Nouvelle Zélande. Ce site est dédié à la veille numérique et la sécurité de l'information

The National White Collar Crime Center: IFCC – Internet fraud complaint Center:
http://www1.ifccfbi.gov/index.asp; Internet Fraud – Crime Report – 2004
http://www1.ifccfbi.gov/strategy/2004_IC3Report.pdf

News Letters

cryptogram de Bruce Schneier [schneier@COUNTERPANE.COM]
CRYPTO-GRAM-LIST@LISTSERV.MODWEST.COM

Info lettre du Forum des droits sur l'internet
infolettre@listes.foruminternet.org

US-CERT Security Bulletins [security-bulletins@us-cert.gov]
security-bulletins@us-cert.gov

La lettre d'information de cyber police http://cyberpolice.over-blog.com/
cyberpolice.over-blog.com [newsletter@over-blog.com]

Annexe F – Les lignes directrices régissant la sécurité des systèmes et réseaux d'information vers une culture de la sécurité – OCDE –

Préface

Le degré d'utilisation des systèmes et réseaux d'information et l'environnement des technologies de l'information dans son ensemble ont évolué de façon spectaculaire depuis 1992, date à laquelle l'OCDE a rendu publiques ses *Lignes directrices régissant la sécurité des systèmes d'information.* Ces évolutions constantes offrent des avantages significatifs mais requièrent également que les gouvernements, les entreprises, les autres organisations et les utilisateurs individuels qui développent, possèdent, fournissent, gèrent, maintiennent et utilisent les systèmes et réseaux d'information (parties prenantes), portent une bien plus grande attention à la sécurité.

Des ordinateurs personnels toujours plus puissants, des technologies convergentes et la très large utilisation de l'internet ont remplacé ce qui était autrefois des systèmes autonomes aux capacités limitées, dans des réseaux essentiellement fermés. Aujourd'hui, les parties prenantes sont de plus en plus interconnectées et les connexions franchissent les frontières nationales. De surcroît, l'internet est le support d'infrastructures vitales telles que l'énergie, les transports et les activités financières et joue un rôle majeur dans la façon dont les entreprises conduisent leurs activités, dont les gouvernements assurent des services aux citoyens et aux entreprises et dont les citoyens communiquent et échangent des informations. La nature et le type des technologies constituant l'infrastructure des communications et de l'information ont également sensiblement évolué. Le nombre et la nature des dispositifs d'accès à cette infrastructure se sont multipliés et diversifiés pour englober les terminaux d'accès fixes, sans fil et mobiles et une proportion croissante des accès s'effectue par l'intermédiaire de connexions «permanentes». Par voie de conséquence, la nature, le volume et le caractère sensible de l'information échangée ont augmenté de façon significative.

Du fait de leur connectivité croissante, les systèmes et réseaux d'information sont désormais exposés à un nombre croissant et à un éventail plus large de menaces et vulnérabilités, ce qui pose de nouveaux problèmes de sécurité. Les présentes lignes directrices s'adressent donc à l'ensemble des parties renantes à la nouvelle société de l'information, et suggèrent le besoin d'une prise de conscience et d'une compréhension des questions de sécurité accrues, ainsi que la nécessité de développer une «culture de la sécurité».

F.1 Vers une culture de la sécurité

Ces lignes directrices répondent à un environnement en constante évolution en appelant au développement d'une culture de la sécurité – ce qui signifie porter une attention très grande à la sécurité lors du développement des systèmes d'information et des réseaux et adopter de nouveaux modes de pensée et de comportement lors de l'utilisation des systèmes et réseaux d'information et dans le cadre des échanges qui y prennent place. Les lignes directrices marquent une rupture nette avec un temps où la sécurité n'intervenait que trop souvent de façon incidente dans la conception et l'utilisation des réseaux et systèmes d'information. Les parties prenantes sont de plus en plus tributaires des systèmes d'information, des réseaux et des services qui leur sont liés, lesquels doivent tous être fiables et sécurisés. Seule une approche prenant dûment en compte les intérêts de toutes les parties prenantes et la nature des systèmes, réseaux et services connexes peut permettre d'assurer une sécurité efficace.

Chaque partie prenante a un rôle important à jouer pour assurer la sécurité. Les parties prenantes, en fonction de leurs rôles respectifs, doivent être sensibilisées aux risques liés à la sécurité ainsi qu'aux parades appropriées, doivent assumer leurs responsabilités et prendre des mesures de nature à améliorer la sécurité des systèmes et réseaux d'information.

L'instauration d'une culture de la sécurité nécessitera à la fois une impulsion et une large participation et devrait se traduire par une priorité renforcée donnée à la planification et la gestion de la sécurité, ainsi que par une compréhension de l'exigence de sécurité par l'ensemble des participants. Les questions de sécurité doivent être un sujet de préoccupation et de responsabilité à tous les niveaux du gouvernement et des entreprises et pour l'ensemble des parties prenantes. Les présentes lignes directrices offrent un fondement aux efforts en vue d'instaurer une culture de la sécurité dans l'ensemble de la société. Les parties prenantes seront ainsi à même d'agir pour que la sécurité devienne partie intégrante de la conception et de l'utilisation de tous les systèmes et réseaux d'information. Les lignes directrices proposent que toutes les parties prenantes adoptent et encouragent une «culture de la sécurité» qui guide la réflexion, la décision et l'action concernant le fonctionnement des systèmes et réseaux d'information.

F.2 Buts

L'objet des lignes directrices est de:

- Promouvoir parmi l'ensemble des parties prenantes une culture de la sécurité en tant que moyen de protection des systèmes et réseaux d'information.
- Renforcer la sensibilisation aux risques pour les systèmes et réseaux d'information, aux politiques, pratiques, mesures et procédures disponibles pour faire face à ces risques, ainsi qu'à la nécessité de les adopter et de les mettre en œuvre.
- Promouvoir parmi l'ensemble des parties prenantes une plus grande confiance dans les systèmes et réseaux d'information et dans la manière dont ceux-ci sont mis à disposition et utilisés.
- Créer un cadre général de référence qui aide les parties prenantes à comprendre la nature des problèmes liés à la sécurité, et à respecter les valeurs éthiques dans l'élaboration et la mise en œuvre de politiques, pratiques, mesures et procédures cohérentes pour la sécurité des systèmes et réseaux d'information.
- Promouvoir parmi l'ensemble des parties prenantes, la coopération et le partage d'informations appropriés pour l'élaboration et la mise en œuvre des politiques, pratiques, mesures et procédures pour la sécurité.
- Promouvoir la prise en considération de la sécurité en tant qu'objectif important parmi toutes les parties prenantes associées à l'élaboration et la mise en œuvre de normes.

F.3 Principes

Les neuf principes exposés ci-après se complètent et doivent être considérés comme un tout. Ils s'adressent aux parties prenantes à tous les niveaux, y compris politique et opérationnel. Aux termes des lignes directrices, les responsabilités des parties prenantes varient selon le rôle qui est le leur. Toutes les parties prenantes, peuvent être aidées par des actions de sensibilisation, d'éducation, de partage d'informations et de formation de nature à faciliter une meilleure compréhension des questions de sécurité et l'adoption de meilleures pratiques en ce domaine. Les efforts visant à renforcer la sécurité des systèmes et réseaux d'information doivent respecter les valeurs d'une société démocratique, en particulier le besoin d'une circulation libre et ouverte de l'information ainsi que les principes de base de respect de la vie privée des individus[62].

---

62 Outre les présentes lignes directrices sur la sécurité, l'OCDE a élaboré une série de recommandations complémentaires concernant des lignes directrices relatives à d'autres aspects importants de la société mondiale de l'information. Celles-ci visent la vie privée (*Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*, OCDE, 1980) et la cryptographie (Lignes directrices régissant la politique de cryptographie, OCDE, 1997). Les présentes lignes directrices sur la sécurité doivent être lues en parallèle avec ces autres lignes directrices.

1) Sensibilisation

Les parties prenantes doivent être sensibilisées au besoin d'assurer la sécurité des systèmes et réseaux d'information et aux actions qu'elles peuvent entreprendre pour renforcer la sécurité.

La sensibilisation aux risques et aux parades disponibles est la première ligne de défense pour assurer la sécurité des systèmes et réseaux d'information. Les systèmes et réseaux d'information peuvent être exposés à des risques tant internes qu'externes. Les parties prenantes doivent comprendre que les défaillances de sécurité peuvent gravement porter atteinte aux systèmes et réseaux sous leur contrôle mais aussi, du fait de l'interconnectivité et de l'interdépendance, à ceux d'autrui. Les parties prenantes doivent réfléchir à la configuration de leur système, aux mises à jour disponibles pour ce dernier, à la place qu'il occupe dans les réseaux, aux bonnes pratiques qu'elles peuvent mettre en œuvre pour renforcer la sécurité, ainsi qu'aux besoins des autres parties prenantes.

2) Responsabilité

Les parties prenantes sont responsables de la sécurité des systèmes et réseaux d'information.

Les parties prenantes sont tributaires de systèmes et réseaux d'information locaux et mondiaux interconnectés. Elles doivent comprendre leur responsabilité dans la sécurité de ces systèmes et réseaux et en être, en fonction du rôle qui est le leur, individuellement comptables. Elles doivent régulièrement examiner et évaluer leurs propres politiques, pratiques, mesures et procédures pour s'assurer qu'elles sont adaptées à leur environnement. Celles qui développent, conçoivent et fournissent des produits et services doivent prendre en compte la sécurité des systèmes et réseaux et diffuser des informations appropriées, notamment des mises à jour en temps opportun de manière à ce que les utilisateurs puissent mieux comprendre les fonctions de sécurité des produits et services et leurs responsabilités en la matière.

3) Réaction

Les parties prenantes doivent agir avec promptitude et dans un esprit de coopération pour prévenir, détecter et répondre aux incidents de sécurité.

Du fait de l'interconnectivité des systèmes et réseaux d'information et de la propension des dommages à se répandre rapidement et massivement, les parties prenantes doivent réagir avec promptitude et dans un esprit de coopération aux incidents de sécurité. Elles doivent échanger leurs informations sur les menaces et vulnérabilités de manière appropriée et mettre en place des procédures pour une coopération rapide et efficace afin de prévenir et détecter les incidents de sécurité et y répondre. Lorsque cela est autorisé, cela peut impliquer des échanges d'informations et une coopération transfrontières.

4) Ethique

Les parties prenantes doivent respecter les intérêts légitimes des autres parties prenantes.

Les systèmes et réseaux d'information sont omniprésents dans nos sociétés et les parties prenantes doivent être conscientes du tort qu'elles peuvent causer à autrui par leur action ou leur inaction. Une conduite éthique est donc indispensable et les parties prenantes doivent s'efforcer d'élaborer et d'adopter des pratiques exemplaires et de promouvoir des comportements qui tiennent compte des impératifs de sécurité et respectent les intérêts légitimes des autres parties prenantes.

5) Démocratie

La sécurité des systèmes et réseaux d'information doit être compatible avec les valeurs fondamentales d'une société démocratique.

La sécurité doit être assurée dans le respect des valeurs reconnues par les sociétés démocratiques, et notamment la liberté d'échanger des pensées et des idées, la libre circulation de l'information, la confidentialité de l'information et des communications, la protection adéquate des informations de caractère personnel, l'ouverture et la transparence.

6) Evaluation des risques

Les parties prenantes doivent procéder à des évaluations des risques.

L'évaluation des risques permet de déceler les menaces et vulnérabilités et doit être suffisamment large pour couvrir l'ensemble des principaux facteurs internes et externes, tels la technologie, les facteurs physiques et humains, les politiques et services de tierces parties ayant des implications sur la sécurité. L'évaluation des risques permettra de déterminer le niveau acceptable de risque et facilitera la sélection de mesures de contrôles appropriées pour gérer le risque de préjudices possibles pour les systèmes et réseaux d'information compte tenu de la nature et de l'importance de l'information à protéger. L'évaluation des risques doit tenir compte des préjudices aux intérêts d'autrui ou causés par autrui rendus possibles par l'interconnexion croissante des systèmes d'information.

7) Conception et mise en œuvre de la sécurité

Les parties prenantes doivent intégrer la sécurité en tant qu'un élément essentiel des systèmes et réseaux d'information.

Les systèmes, réseaux et politiques doivent être conçus, mis en œuvre et coordonnés de façon appropriée afin d'optimiser la sécurité. Un axe majeur, mais non exclusif, de cet effort doit être la conception et l'adoption de mesures de protection et solutions appropriées afin de prévenir ou limiter les préjudices possibles liés aux vulnérabilités et menaces identifiées. Les mesures de protection et solutions doivent être à la fois techniques et non techniques et être proportionnées à la valeur de l'information dans les systèmes et réseaux d'information de l'organisation. La sécurité doit être un élément fondamental de l'ensemble des produits, services, systèmes et réseaux et faire partie intégrante de la conception et de l'architecture des systèmes. Pour l'utilisateur final, la conception et la mise en œuvre de la sécurité consistent essentiellement à sélectionner et configurer des produits et services pour leurs systèmes.

8) Gestion de la sécurité

Les parties prenantes doivent adopter une approche globale de la gestion de la sécurité.

La gestion de la sécurité doit être fondée sur l'évaluation des risques et être dynamique et globale afin de couvrir tous les niveaux d'activités des parties prenantes et tous les aspects de leurs opérations. Elle doit inclure également, par anticipation, des réponses aux menaces émergentes et couvrir la prévention, la détection et la résolution des incidents, la reprise des systèmes, la maintenance permanente, le contrôle et l'audit. Les politiques de sécurité des systèmes et réseaux d'information, les pratiques, mesures et procédures en matière de sécurité doivent être coordonnées et intégrées pour créer un système cohérent de sécurité. Les exigences de la gestion de la sécurité sont fonction du niveau de participation, du rôle de la partie prenante, des risques en jeu et des caractéristiques du système.

9) Réévaluation

Les parties prenantes doivent examiner et réévaluer la sécurité des systèmes et réseaux d'information et introduire les modifications appropriées dans leurs politiques, pratiques, mesures et procédures de sécurité.

Des vulnérabilités et menaces nouvelles ou évolutives sont constamment découvertes. Toutes les parties prenantes doivent continuellement revoir, réévaluer et modifier tous les aspects de la sécurité pour faire face à ces risques évolutifs.

Recommandation du Conseil concernant les lignes directrices regissant la securité des systèmes et réseaux d'information vers une culture de la securité

LE CONSEIL,

Vu la Convention relative à l'Organisation de Coopération et de Développement Economiques, en date du 14 décembre 1960, et notamment ses articles 1 b), 1 c), 3 a) et 5 b);

Vu la Recommandation du Conseil concernant les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel, en date du 23 septembre 1980 [C(80)58(Final)];

Vu la Déclaration sur les flux transfrontières de données adoptée par les gouvernements des pays Membres de l'OCDE le 11 avril 1985 [C(85)139,Annexe];

Vu la Recommandation du Conseil relative aux Lignes directrices régissant la politique de cryptographie, en date du 27 mars 1997 [C(97)62/FINAL];

Vu la Déclaration ministérielle relative à la protection de la vie privée sur les réseaux mondiaux, en date des 7-9 décembre 1998 [C(98)177/FINAL, Annexe];

Vu la Déclaration ministérielle sur l'authentification pour le commerce électronique, en date des 7-9 décembre 1998 [C(98)177/FINAL, Annexe];

Reconnaissant que les systèmes et réseaux d'information sont de plus en plus utilisés et acquièrent une valeur croissante pour les gouvernements, les entreprises, les autres organisations, et les utilisateurs individuels;

Reconnaissant que le rôle toujours plus important que jouent les systèmes et réseaux d'information dans la stabilité et l'efficience des économies nationales et des échanges internationaux, ainsi que dans la vie sociale, culturelle et politique, et l'accentuation de la dépendance à leur égard imposent des efforts particuliers pour protéger et promouvoir la confiance qui les entoure;

Reconnaissant que les systèmes et réseaux d'information et leur expansion à l'échelle mondiale se sont accompagnés de risques nouveaux et en nombre croissant;

Reconnaissant que les données et informations conservées ou transmises sur des systèmes et réseaux d'information sont exposées à des menaces du fait de divers moyens d'accès sans autorisation, d'utilisation, d'appropriation abusive, d'altération, de transmission de code malveillant, de déni de service ou de destruction, et exigent des mesures de protection appropriées;

Reconnaissant qu'il importe de sensibiliser davantage aux risques pesant sur les systèmes et réseaux d'information ainsi qu'aux politiques, pratiques, mesures et procédures disponibles pour faire face à ces risques, et d'encourager des comportements appropriés en ce qu'ils constituent une étape essentielle dans le développement d'une culture de la sécurité;

Reconnaissant qu'il convient de revoir les politiques, pratiques, mesures et procédures actuelles pour aider à faire en sorte qu'elles répondent de façon adéquate aux défis en constante évolution que posent les menaces auxquelles sont exposés les systèmes et réseaux d'information;

Reconnaissant qu'il est de l'intérêt commun de promouvoir la sécurité des systèmes et réseaux d'information par une culture de la sécurité qui encourage une coordination et une coopération internationales appropriées en vue de répondre aux défis posés par les préjudices que des défaillances de la sécurité sont susceptibles de causer aux économies nationales, aux échanges internationaux, ainsi qu'à la participation à la vie sociale, culturelle et politique.

Reconnaissant en outre que les *Lignes directrices régissant la sécurité des systèmes et réseaux d'information: vers une culture de la sécurité*, figurant en annexe à la présente Recommandation, sont d'application volontaire et n'affectent pas les droits souverains des Etats;

Et reconnaissant que l'objet de ces lignes directrices n'est pas de suggérer qu'il existe une solution unique quelconque en matière de sécurité, ou que des politiques, pratiques, mesures et procédures particulières soient adaptées à une situation donnée, mais plutôt de fournir un cadre plus général de principes de nature à favoriser une meilleure compréhension de la manière dont les parties prenantes peuvent à la fois bénéficier du développement d'une culture de la sécurité et y contribuer;

PRÉCONISE l'application de ces *Lignes directrices régissant la sécurité des systèmes et réseaux d'information: vers une culture de la sécurité* par les gouvernements, les entreprises, les autres organisations et les utilisateurs individuels qui développent, possèdent, fournissent, gèrent, maintiennent et utilisent les systèmes et réseaux d'information;

RECOMMANDE aux pays Membres:

D'établir de nouvelles politiques, pratiques, mesures et procédures ou de modifier celles qui existent pour refléter et prendre en compte les *Lignes directrices régissant la sécurité des systèmes et réseaux d'information: vers une culture de la sécurité* en adoptant et promouvant une culture de la sécurité, conformément auxdites lignes directrices;

D'engager des actions de consultation, de coordination et de coopération, aux plans national et international, pour la mise en œuvre des lignes directrices;

De diffuser les lignes directrices dans l'ensemble des secteurs public et privé, notamment auprès des gouvernements, des entreprises, d'autres organisations et des utilisateurs individuels, pour promouvoir une culture de la sécurité, et encourager toutes les parties intéressées à adopter une attitude responsable et à prendre les mesures nécessaires en fonction des rôles qui sont les leurs;

De mettre les lignes directrices à la disposition des pays non membres, le plus rapidement possible et de manière appropriée;

De réexaminer les lignes directrices tous les cinq ans, de manière à promouvoir une coopération internationale sur les questions liées à la sécurité des systèmes et réseaux d'information;

CHARGE le Comité de la politique de l'information, de l'informatique et des communications de l'OCDE d'apporter son soutien à la mise en œuvre des lignes directrices.

La présente Recommandation remplace la Recommandation du Conseil concernant les lignes directrices régissant la sécurité des systèmes d'information du 26 novembre 1992 [C(92)188/FINAL].

Historique de la procédure

Les lignes directrices sur la sécurité ont été achevées en 1992 puis réexaminées en 1997. L'examen actuel a été entrepris en 2001 par le Groupe de travail sur la sécurité de l'information et la vie privée (GTSIVP), dans le cadre d'un mandat donné par le Comité de la politique de l'information, de l'informatique et des communications (PIIC), et accéléré suite à la tragédie du 11 septembre.

La rédaction a été entreprise par un Groupe d'experts du GTSIVP qui s'est réuni à Washington, DC, les 10 et 11 décembre 2001, à Sydney les 12-13 février 2002 et à Paris les 4 et 6 mars 2002. Le GTSIVP s'est réuni les 5-6 mars 2002, les 22-23 avril 2002 et les 25-26 juin 2002.

Les présentes *Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information: vers une culture de la sécurité* ont été adoptées sous la forme d'une Recommandation du Conseil de l'OCDE lors de sa 1037^{e} session, le 25 juillet 2002.

Union internationale des télécommunications
Bureau de développement des télécommunications (BDT)
Place des Nations
CH-1211 Genève 20
Suisse

Pour plus d'information, veuillez contacter:
Alexander NTOKO
Chef, Unité Cyberstratégies
E-mail: e-strategies@itu.int
Site Web: www.itu.int/ITU-D/e-strategies

Imprimé en Suisse
Genève, 2006