Livre Blanc du Groupe 4

Sécurité des Systèmes d'Information

Directeur Pôle Sécurité des Systèmes d'Information au Groupe 4
Bruno DOUCENDE

Copyright

Mention sur les droits restreints

Marques commerciales et de service

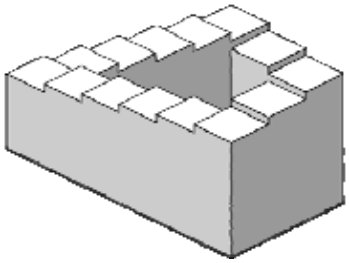
CWP1567D1252-1A

Avant Propos

La sécurité des systèmes informatiques et plus globalement des systèmes d'information (SI) a été considéré pendant très longtemps par les entreprises, comme un aspect de second plan. Peu à peu, une prise de conscience amène la Sécurité des SI sur le devant de la scène. La raison principale est liée à la multitude d'incidents et plus grave, de sinistres qui provoquent de lourdes pertes aussi bien pour les entreprises que pour le simple citoyen.

Mais le chemin est encore long pour que la Sécurité des SI soit une véritable réalité dans les organismes et les entreprises petites, moyennes ou grandes.

Encore trop souvent, j'entends dire « *Mon entreprise est sécurisée car elle dispose d'un firewall et d'un antivirus* ». Si cela est un bon début, il ne s'agit que des premières marches de l'immense escalier de la Politique de Sécurité des SI, que l'on pourrait comparer à l'escalier infini du mathématicien Penrose. La sécurité des systèmes d'information est un (très) vaste domaine en perpétuelle évolution.



L'escalier de Penrose
illustration : Philip Ronan

Malheureusement la sécurité est appréhendée correctement après un sinistre important.

« *La sécurité a un coût* », me dit-on.

Je réponds : « *Exact ! Mais la non-sécurité a également un coût*.»

Plus généralement, le système d'information a un coût. Mais bien conçu, bien utilisé le système d'information s'avère être un atout de performance pour un organisme. On associe alors, Système d'information et gain de productivité.

La vision de la Sécurité des SI doit être semblable, au détail près qu'elle n'engendre pas de gain en premier lieu, mais elle évite des pertes (liées à un sinistre). Bien appréhendée, la sécurité des SI ou plus simplement la sécurité de l'information, peut apporter un avantage concurrentiel. L'approche de la Sécurité de l'information est donc un **enjeu financier et même stratégique pour les organismes**.

Il faut donc penser et concevoir la Sécurité des systèmes d'information comme un investissement. Et en cela, c'est un véritable chantier.

C'est l'objectif de ce livre blanc : **Faire prendre conscience** de l'enjeu sécuritaire et présenter dans ses grandes lignes, les contours d'une approche gagnante de la Sécurité des SI. Ainsi dans cette perspective**, sensibiliser** et **former** l'ensemble des acteurs de l'entreprise et des organismes, est une première pierre à l'édifice.

Naturellement ce livre blanc est une synthèse et de fait n'est pas exhaustif. Le terme générique d'Organisme sera employé pour désigner globalement les entreprises, organisations, administrations, collectivités territoriales, … .

A Propos de l'Auteur

Bruno DOUCENDE est Consultant indépendant spécialisé en Sécurité des Systèmes d'information.

Ingénieur en Informatique EFREI, après plusieurs années en Société de Service en tant qu'Ingénieur d'Etudes & Développement et Chef de Projet, Bruno DOUCENDE a pris en charge, la direction d'unités de Recherche & Développement en conception logicielle et en exploitation d'infrastructures dans le domaine des systèmes d'information et des NTIC.

Il a assuré des missions à responsabilité opérationnelle, d'organisation, de pilotage, d'audit, de stratégie & conseil, et de management dans la conception, le développement et l'exploitation de systèmes d'information pour divers secteurs d'activités : le médical, les transports, les administrations, collectivités locales, l'Aéronautique, Industrie, Les sociétés de services, ...

Ces expériences l'ont amené à être en permanence au contact des problématiques et besoins des entreprises et ainsi appréhender et participer à leur stratégie globale dans un contexte concurrentiel, où la sécurisation de leur Système d'Information constitue un enjeu majeur.

Fort de ces expériences professionnelles réussies, Bruno Doucende accompagne aujourd'hui les sociétés, en tant que consultant sous l'enseigne Synertic Conseil.

Il anime des séminaires sur la sécurité des systèmes d'information en France et à l'International, auprès des petites, moyennes et grandes entreprises, administrations et ministères. Il les accompagne et les assiste dans l'élaboration et le suivi de leur politique de sécurité des SI.

Au sein des Ecoles d'Ingénieur-Manager et Centre de Formation du Groupe 4, Bruno DOUCENDE a pris en charge le pôle Sécurité des SI et intervient comme enseignant dans les domaines de la Sécurité des Systèmes d'Information, du Management de la Qualité, de l'Intelligence Economique. Il fait également parti des consultants qui encadrent et assurent le suivi des projets « Sim Game », mettant en situation réelle un projet d'envergure, sur un système d'information avec des équipes de 20 à 50 personnes durant plusieurs mois.

Sommaire

Contexte 6

La sécurité des SI : Effet Marketing ou Réel Besoin? 9

L'homme : le maillon faible 13

Les codes malicieux : Véritable pandémie 16

Vulnérabilité et Intrusion : le vol à l'étalage 18

La protection de l'information 19

Les aspects juridiques 21

Concevoir des solutions sécurisées : Une nécessité 22

Management de la sécurité : une vision globale 25

De la Protection à la Maitrise Stratégique de l'Information 28

Le RSSI : une compétence transverse, un rôle stratégique 29

Conclusion : « La Sécurité, c'est l'affaire de tous ! » 30

Contexte

La société de l'information : Une évidence

Une information est une donnée qui a un sens. En fonction d'un modèle d'interprétation, une donnée constitue une signification pour une personne au moment où celle-ci va en prendre connaissance.

Une information peut apporter à celui qui la détient un avantage substantiel. On parle alors de valeur de l'information. Quelque soit les domaines, la connaissance ou la maitrise de l'information peut s'avérer un atout décisif.

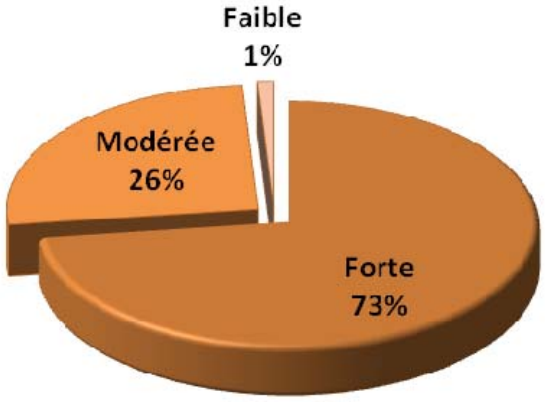
Cela est vrai depuis la nuit des temps. Mais aujourd'hui, grâce à l'essor des technologies de l'information et de la communication, la gestion de l'information devient plus aisée et plus efficiente.

Aujourd'hui, qui pourrait nier l'omniprésence de l'outil informatique dans nos quotidiens, que ce soit dans le domaine professionnel ou à la maison.

L'environnement et les outils numériques se sont propagés partout, la simplicité et la facilité d'accès et de manipulation de l'information, sous toutes ses formes, est une réalité.

L'outil informatique a permis d'optimiser l'acquisition, le traitement et la production d'information. L'interconnexion des systèmes et le développement des réseaux a complété les possibilités de partage, de diffusion et de communication de cette information.

Bien évidement, l'activité économique n'y a pas échappée. Si bien que la majorité des entreprises ne peuvent plus se passer de leur système d'information.



Dépendance des entreprises vis-à-vis de leur Système d'Information (Clusif 2008)

Les systèmes d'Information : Un atout majeur

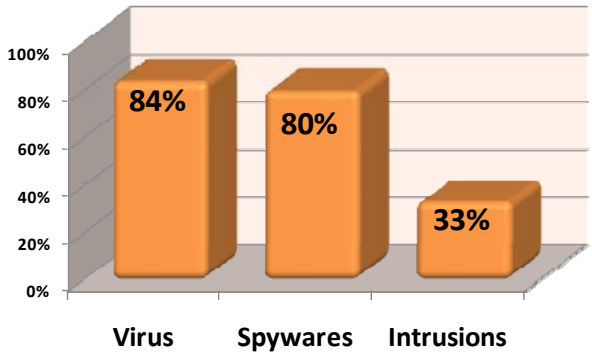
Dans le contexte de mondialisation où la concurrence est âpre, pour assoir leur position les entreprises sont en quête de compétitivité, de productivité. Pour répondre à ces nécessités, les technologies de l'information et de la communication, sont devenues incontournables dans le quotidien des entreprises. La maitrise et la réactivité de l'information constituent un avantage stratégique. Les systèmes d'informations sont un enjeu, un défi pour les entreprises, organismes et administrations. Ainsi les Systèmes d'Information ont un périmètre fonctionnel de plus en plus large et complexe avec une exigence d'adaptation et d'évolutivité très importante et véloce.

Si les technologies de l'Information et de la communication sont aujourd'hui un facteur de progrès et de croissance incontestable pour les entreprises, elles sont aussi leur talon d'Achille. Une dépendance trop forte et une complexité non maîtrisée, sont synonymes de faiblesse potentielle, si elles ne sont pas gérées.

L'insécurité des SI : Des exemples à foisons

Grâce aux medias ou tout simplement à travers des expériences autour de nous, les exemples de malveillance visant les systèmes d'information sont nombreux :

- Les ordinateurs incontrôlables et inutilisables à cause de virus informatiques.
- L'intrusion par un pirate dans un réseau engendrant le vol d'informations.
- Le nombre de sites web défigurés par des groupes de «cyber-tagueurs».
- Les logiciels espions (spyware) installés discrètement sur nos ordinateurs pour épier nos habitudes, nos comportements, nos données.



Répartition des d'attaques subies par les entreprises (FBI : 2005)

Au-delà de la malveillance, un autre aspect, à ne pas omettre, concerne les défaillances du système d'information, à cause de pannes, de mauvaises utilisations ou catastrophes naturelles, les rendant totalement ou partiellement inutilisables.

Tous ces exemples peuvent avoir des conséquences graves voire vitales pour tout organisme. Il y a encore quelques années, cette insécurité des SI avait des conséquences limitées, mais aujourd'hui nous sommes entrés dans « l'ère industrielle ». Effectivement, les attaquants cherchent désormais à « monétiser » leurs méfaits.

90% des sociétés ont subi au moins une attaque, dont 20% ont provoqué un sabotage de données.
(FBI : 2005)

Nous sommes passés des bandits de grands chemins aux organisations criminelles structurées et déterminées à exploiter pleinement le potentiel des autoroutes de l'information.

La cybercriminalité : Mutation des crimes et délits

Toute activité, toute innovation synonyme de progrès, peut engendrer aussi des comportements illicites. Le domaine des technologies de l'information et de la communication n'y échappe pas.

En 2005, selon une enquête du FBI, le cout de la cybercriminalité aux USA a représenté plus de **67 milliard de dollars.**

Ainsi, la cybercriminalité est une application et adaptation des crimes à travers les nouvelles technologies, dont les conséquences peuvent être particulièrement sérieuses pour la sécurité des citoyens et des activités économiques. Les atteintes peuvent porter sur le plan de la dignité, du patrimoine et de la liberté individuelle.

La délinquance a toujours existé et s'est toujours adaptée aux différents espaces (terrestre, maritime, aérien). Aujourd'hui avec les technologies de l'information et de la communication, un nouvel espace est disponible. L'espace informationnel. La caractéristique de cet espace est la dématérialisation, le caractère pseudo-virtuel et la capacité à être en relation instantanément avec potentiellement plus d'un milliard d'internautes en un clic de souris.

De ce fait, un sentiment de virtualisation incite certains, à franchir aisément les barrières légales et morales qu'ils n'auraient certainement pas franchir dans les autres espaces.

De plus, la facilité d'agresser une multitude de proies presque en simultané, démontre que cette délinquance a un potentiel de nuisance très considérable.

La cybercriminalité se définit comme tous les types de délits perpétrés à travers ou à l'aide d'internet ou autres réseaux de télécommunications. Elle se caractérise par trois types d'infractions :

- Les infractions relatives au contenu (insultes, xénophobie, pédophilie, …).
- Les infractions relatives à la propriété intellectuelle (musique, vidéo, logiciel, …).
- Les infractions spécifiques aux Technologie de l'Information et à la Communication (virus, vol de données, escroquerie en ligne, …).

Les proies, utilisatrices des réseaux de télécommunications, sont multiples : le simple particulier, les enfants, les organismes, les entreprises et les Etats. D'ailleurs les états ont pris conscience de ce fléau et adaptent leur politique de sécurisation.

Face à ce tableau plutôt noir, un élément est plutôt positif, malgré le pseudo anonymat perçu par certains délinquants, les systèmes d'information et les technologies peuvent générer des traces, des empreintes numériques et servir de « réservoir » de preuves, indispensables pour les enquêtes et éventuelles poursuites… à condition d'avoir mis en œuvre ces « réservoirs » !

La sécurité des SI : Effet Marketing ou Réel Besoin?

Comme nous l'avons vu précédemment, les systèmes d'information sont devenus un des éléments névralgiques dans le fonctionnement et la performance des divers organismes (Entreprises, administrations, …). De ce fait, en cas de défaillance totale ou même partielle le fonctionnement de l'organisme sera fortement perturbé.

En juillet 2008, une carte réseau défectueuse du système de la tour de contrôle a engendré la fermeture temporaire de l'aéroport de Dublin.

De plus, le système d'information renferme des données précieuses, certaines de ces données sont propres à l'entreprise, d'autres concernent des tiers comme les clients, les partenaires,… Ainsi, la perte ou l'altération de ces données peut constituer un préjudice parfois fatal. En complément, dans un contexte de plus en plus concurrentiel, l'information représente une valeur et donc une convoitise. Ces données peuvent être dérobées sans que personne s'en aperçoive, même à postériori, à la différence d'un vol d'un porte monnaie par exemple.
Imaginez les conséquences si un concurrent pouvait accéder, en toute discrétion, aux données de la politique tarifaire d'une entreprise. Malheureusement ce type de situation n'est pas de la fiction !

Compte tenu de l'enjeu économique et financier, cette forme de criminalité s'est développée ces dernières années, à tel point que pour certaine organisation mafieuse, cette opportunité devient plus rentable que le commerce de la drogue. Sur l'échelle de la maturité, ce type de criminalité est à l'âge de l'adolescence. Outre les supports actuels, l'essor prochain de l'ultra-mobilité, la convergence de la voix, l'image, de la domotique, les puces à radio fréquence, les nanotechnologies, … offrent un terreau prolifique.

Ainsi, pour les entreprises et organismes, petites ou grandes, prendre en compte ces risques notoires en perpétuelle évolution, est donc devenu une nécessité. C'est une question **sinon de survie, au moins d'efficience**.

L'élaboration d'une politique de sécurité est une obligation. Mais cette élaboration ne doit pas rester un alibi pour se donner bonne conscience. L'objectif réside dans la pertinence et la mise en pratique de processus orientés Sécurité du SI. C'est-à-dire appliquer et faire appliquer une politique sécurité en phase avec le contexte de l'organisme.

Les défaillances en matière de sécurité d'un système (cela est vrai quelque soit le domaine), résultent de la conjonction simultanée ou séparée de deux facteurs :

1. **L'erreur humaine** quelle soit volontaire ou non.
2. **Les faiblesses du système** sous forme d'anomalies ou de défauts d'entretien.

Par analogie, on peut transposer ce constat, dans le domaine de la sécurité routière, où l'accident peut être causé par :

1. l'inattention, le laxisme, l'indiscipline ou l'incompétence du chauffeur.
2. le défaut du véhicule suite à une anomalie, une négligence d'entretien, ou du mauvais état de la route ou de la signalisation.

N'oublions pas que, sur la route, on peut être victime d'un accident à cause de l'erreur d'un autre chauffeur que l'on a croisé au mauvais moment au mauvais endroit. En matière de sécurité des Systèmes d'Information, on peut également être une victime de la négligence d'autrui !

Contrairement aux idées reçues, la sécurisation d'un système d'information d'un organisme ne consiste pas à mettre uniquement en œuvre une forteresse technique pour empêcher les «assaillants» externes d'y pénétrer. Si cela est forcement nécessaire, elle n'est pas suffisante car 80% des problèmes de sécurité des systèmes d'information proviennent de l'intérieur des organismes. Paradoxalement, le maillon faible en terme de sécurité informatique, est l'homme.

En matière de Sécurité, le risque zéro n'existe pas et aucune protection n'est infaillible. L'objectif de la sécurisation est donc la prise de conscience du risque, son évaluation et la mise en œuvre de parades pour le minimiser.

Objectifs

Il convient de rappeler les cinq objectifs de la sécurité des systèmes d'information :

- **l'authentification**, permettant de vérifier qu'une entité est bien celle qu'elle prétend être
- **l'intégrité**, c'est-à-dire garantir que les données sont bien celles qu'on croit être
- **la confidentialité**, consistant à assurer que seules les entités autorisées aient accès aux ressources
- **la non répudiation**, permettant d'éviter à une entité de pouvoir nier avoir pris part à une action
- **la disponibilité** et la **continuité de service**, permettant de maintenir le bon fonctionnement des systèmes

Une politique de sécurisation doit associer sensibilisation, rigueur, technique, organisation, procédures, surveillance, ...

Une politique de sécurité n'est jamais définitive face à des risques et aux organismes qui sont en perpétuelle évolution.

La sécurisation d'un système d'information est donc indispensable pour la protection du patrimoine et de l'image d'un organisme. La

sécurisation des systèmes d'information consiste à mettre en place les protections nécessaires contre les **dommages subis ou causés** par l'outil informatique et découlant de l'acte volontaire, involontaire ou malveillant d'un individu, qu'il soit externe ou interne à l'organisme.

Menaces et Modes Opératoires

En matière de sécurité des Système d'Information, on dénombre sept menaces. Trois menaces concernent directement l'information :

- **Perte et destruction de données.**
- **Modification de données.**
- **Interception de données** (vol et espionnage).

Dans **9 cas sur 10,** la perte totale des données entraîne la fermeture de l'entreprise.

La quatrième menace concerne la continuité des process :

- **Indisponibilité des systèmes.**

Les trois menaces suivantes sont souvent oubliées mais sont tout aussi importantes :

- **Dégradation de l'image** de marque.
- **Détournement d'activité** via les technologies de l'Information et de la communication.
- **Sanctions juridiques** pour défaut de protection de données des tiers ou utilisation prohibée (même involontaire) des technologies, par les membres d'une entreprise.

Ces menaces sont générées par une multitude de modes opératoires. Un mode opératoire peut d'ailleurs engendrer plusieurs menaces simultanément.

Les vecteurs opératoires de ces menaces sont de plus en plus nombreux avec une forte progression ces dernières années. Virus, Spyware, Botnets, Troyens, Vers, Hoax, Phishing, Ingénierie sociale (arnaques), Scam, Intrusions, Piratage, Typosquatting, Défaillance, Incendies, Catastrophe naturelles, Mauvaise utilisation, … en sont quelques aperçus dont certains seront détaillés dans les pages suivantes.

Les ennemis

On compare souvent la lutte contre la malveillance sur les systèmes d'information comme une guerre. Et comme le disait Sun Tzu, philosophe chinois du Vème siècle Av JC, pour gagner une bataille, il faut bien connaitre son ennemi et ses intentions éventuelles.

Concernant les systèmes d'information, on peut lister quelques ennemis potentiels :

- Le pirate ou l'espion qui agit à des fins pécuniaires ou idéologiques :
  - Organisations criminelles, Mafias, Groupes terroristes.
  - Organisations étatiques.
  - Sociétés spécialisés dans le renseignement économique.

- Le pirate ludique qui va œuvrer par plaisir intellectuel
- Les Scripts Kiddies ou pirates débutants, souvent des adolescents, qui vont « tester des attaques » qu'ils ont découvert par exemple sur internet
- L'employé mécontent de ne pas avoir obtenu ce qu'il voulait
- …

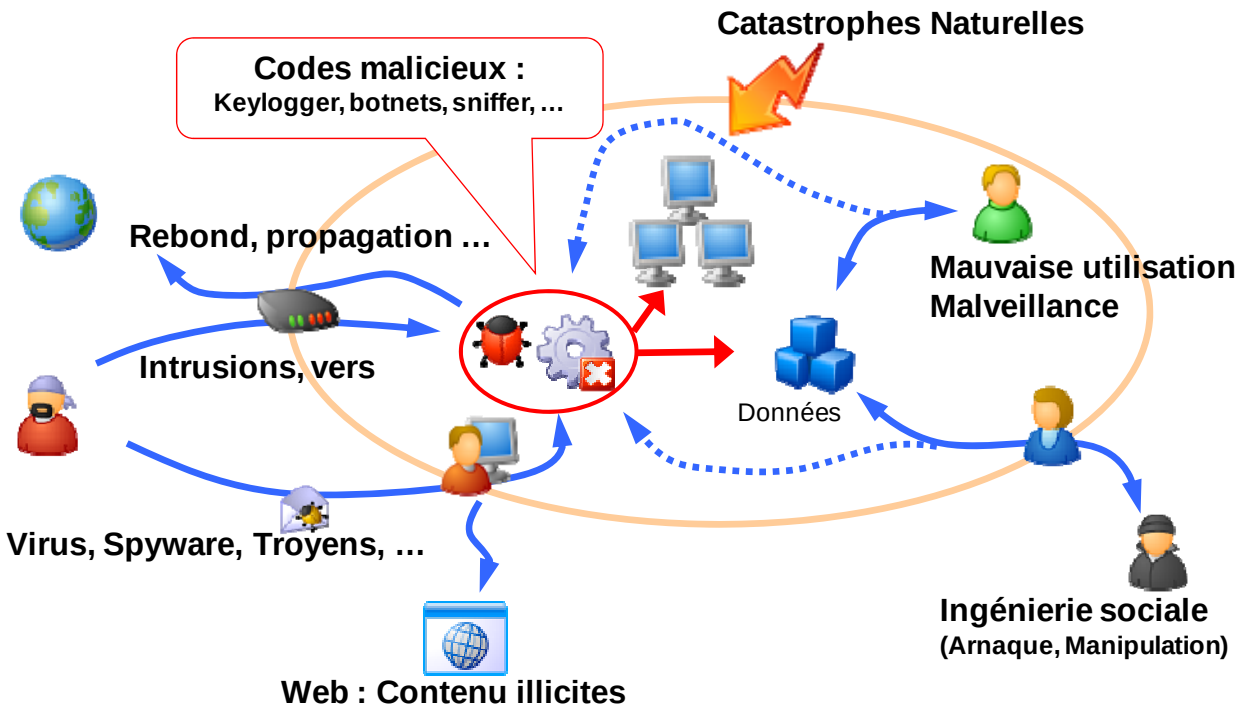
Leurs objectifs sont multiples :

- Désinformer ou Déstabiliser, Récupérer des informations.
- Frauder, mettre en œuvre des arnaques, Manipuler.
- Empêcher l'accès à une ressource, Saboter les données ou les systèmes.
- Prendre le contrôle d'un système, Utiliser un système pour « rebondir » et attaquer un autre système.

Les types d'attaques

Dans le cadre d'un organisme, nous pouvons cartographier les attaques ou modes opératoires en six principales familles :

- Pannes, Accidents, catastrophe naturelles, vol de ressources matérielles.
- Mauvaise utilisation ou malveillance des employés.
- Manipulation des employés par ingénierie sociale.
- Code malicieux.
- Intrusion, rebond et propagation.
- Accès à du contenu illicites.



L'homme : le maillon faible

L'évolution et la mise en place de solutions techniques de sécurité rendent la tâche des pirates de plus en plus complexe pour pénétrer dans les systèmes d'information. Ainsi, il est plus simple pour eux de solliciter un utilisateur de ce système d'information, de le manipuler (ou l'arnaquer) afin que cet utilisateur puisse l'aider involontairement à contourner les dispositifs de sécurité. C'est ce que l'on appelle **l'Ingénierie sociale**.

Nous pouvons élaborer la meilleure politique de sécurité, en terme technique, organisationnelle, si les utilisateurs sont négligents et non sensibilisés aux risques, notre politique de sécurité s'effondre.

L'ingénierie sociale est donc l'art de l'arnaque, qui consiste à manipuler les personnes afin de court-circuiter les dispositifs de sécurité. L'ingénierie sociale utilise des prédispositions humaines qui sont :

- les attitudes naturelles comme le laxisme, le choix du moindre effort, …
- l'attirance naturelle telle que les jeux, le charme, le sport, …
- les tendances psychologiques de la nature humaine vis-à-vis de l'autorité : (intimidation, dangers, culpabilité …), la sympathie (compassion, points communs,…), la réciprocité, la cohérence (basée sur un langage commun)

Mode d'attaque

La mise en œuvre d'une technique d''ingénierie sociale nécessite trois éléments :

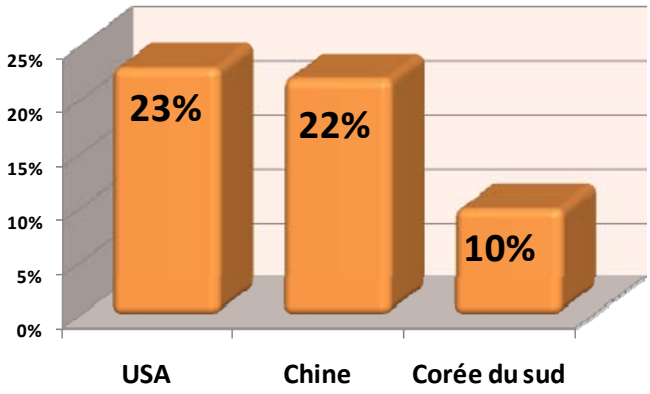
1. Une **phase de renseignement** effectuée par l'attaquant pour identifier et cerner l'angle d'attaque de la ou les victimes. Cette phase est souvent facilitée par la victime elle-même (blog, site web, interview dans la presse,…).
2. **L'usurpation d'identité** où l'attaquant se fait passer auprès de la victime pour une autre personne ou entité (connue ou identifiée par la victime).
3. **La manipulation** elle-même en usant les leviers psychologiques : Manque d'affection, bons sentiments, peur, égo, appât du gain, penchants spécifiques, …

Différentes techniques

La phase d'usurpation d'identité est mise en œuvre par une prise de contact par divers moyens : téléphone, rencontre directe ou par mail, notamment à l'aide du SPAM.

Le **SPAM**, ou envoi massif de courriers indésirables, présente des contenus très variés, principalement pour des sollicitations commerciales. Au delà de l'aspect « qualitatif » des produits proposés, cela constitue une véritable problématique d'engorgement des

serveurs et messagerie et des boites aux lettres. La Facture est estimée à plus de 10 milliard d'€. Le SPAM est aussi utilisé dans le cheminement de code malicieux et la phase de prise de contact dans l'ingénierie sociale. Les techniques les plus utilisées, pour contacter les utilisateurs futurs victimes, sont variés. Voici quelques modes :



Top 3 : Provenance des SPAM

Le Phishing. A travers un e-mail d'un faux expéditeur (usurpation de marque, par exemple une banque) l'objectif est de proposer au destinataire un lien hypertexte pour l'emmener vers un site web falsifié, afin de lui dérober son identifiant et mot de passe. Cette technique est très prisée pour détourner des sommes par virement.
Depuis peu, cette technique s'adapte puisque le site web falsifié est remplacé par un faux serveur vocal. On parle ici de Vishing (Contraction du VoIP et Phishing).

Le Scam connu sous la dénomination de SPAM Nigéria : le but est d'extorquer des fonds en faisant miroiter de l'argent. Par exemple une demande d'aide (contre récompense) au rapatriement de plusieurs millions d'euros ou une notification annonçant que vous êtes l'heureux gagnant à une loterie.

Un gérant d'un cybercafé Camerounais, responsable d'un réseau de SCAM est interpellé en 2006 après les plaintes de plusieurs victimes françaises, pour un préjudice de **500 000 €**.

Dans ces cas, l'attaquant va recruter un deuxième profil de victime, ce que l'on appelle des **mules**, pour répondre à une problématique : Comment récupérer les fonds illégalement acquis par phishing, scam, ou autre en brouillant les pistes d'une éventuelle enquête ? A travers du SPAM, l'attaquant va proposer des « jobs » à des internautes crédules (les mules), pour servir d'intermédiaire des flux financier contre commission.
Il s'agit là d'arnaques à « plusieurs étages », où leurs auteurs font preuve de beaucoup d'ingéniosité.

Le Mot de Passe: le premier rempart

Très souvent, les auteurs d'ingénierie sociale, cherchent à obtenir le mot de passe d'un utilisateur. Ce sésame lui permettra de pénétrer dans le système d'information.

Effectivement, l'accès à un système d'information requiert une authentification. Aujourd'hui, l'utilisation d'un login (identifiant) et mot de passe est encore le système d'authentification plus répandu. Le mot de passe revêt donc une dimension particulière en matière de sécurité. De fait, il existe des techniques et outils permettant de « dérober », découvrir (ou cracker) un mot de passe :

- **Attaque par force brute** : Tester toutes les combinaisons possibles.
- **Attaque par dictionnaire** : Tester des mots et combinaisons de mots usuels (nom commun et nom propre).
- **Keylogger** programme malicieux qui enregistre les touches saisies sur un clavier.
- **Sniffer** programme malicieux qui écoute les transmissions d'un réseau.

Ainsi, le canal d'échange par lequel transite les mots de passe, doit être sécurisé (crypté) et le contexte de saisie garanti (antivirus contre les keylogger). Les trois règles importantes de gestion d'un mot de passe sont :

- **Complexité** : nombre de caractères élevé, caractères étendus (chiffres, signes, majuscule, miniscule,…). Eviter de choisir le login, le nom, prénom (personnel ou d'un proche), un mot à l'envers, un mot suivi de l'année en cours ou d'une année de naissance, …
- **Changement régulier** du mot de passe.
- Utilisation de **plusieurs mots de passe** selon le niveau de confidentialité voulu.

Moyens de Prévention

Les attaquants exploitent le manque de connaissances des utilisateurs pour contourner les dispositifs de sécurité. Il faut donc vis-à-vis de l'ensemble des collaborateurs d'un organisme (employés, stagiaires, sous traitant, …) :

- Les sensibiliser et les former vis-à-vis des risques et enjeux.
- Mettre en place une Charte d'utilisation, règlement intérieur de sécurité qui définit les Droits et Devoirs vis-à-vis de l'utilisation du système d'information.
- Mettre en place de procédures notamment pour :
  - L'identification et la vérification des interlocuteurs sollicitant un utilisateur (éviter la confiance spontanée).
  - Faire des comptes-rendus (d'étonnement) vers les supérieurs hiérarchiques.
  - …

En 2008, seulement **38% des entreprises** communiquent sur la sécurité.

50 % d'entreprises déclarent disposer d'une charte sécurité.

D'autre part, la mise en place de solutions de filtrage d'emails ou Antispam devient indispensable au sein des entreprises et même au niveau des particuliers. Elles permettent d'une part de bloquer souvent les sollicitations malveillantes mais également d'éviter l'engorgement de la messagerie.

Les codes malicieux : Véritable pandémie

La problématique des codes malicieux, terme générique regroupant les logiciels de type virus, spyware, cheval de Troie et autres, est connue de tous. L'insécurité informatique est souvent associée à Virus. Les codes malicieux sont des programmes logiciels dont le but est de nuire. Il s'agit là du risque premier en terme d'attaque. Leur nombre a considérablement augmenté ces dernières années et ils sont de plus en plus dangereux.

Les codes malicieux s'attaquent à toutes les plates formes systèmes (Windows, Linux, Mac OS, …) ainsi que les PDA (agendas électroniques), Smartphones (téléphones portables), consoles de jeux, …

Autre tendance, sur le plan technique, les nouveaux logiciels malicieux sont de plus en plus polymorphes, c'est-à-dire qu'ils changent leur code chaque fois qu'ils sont activés (exécutés), ce qui rend la lutte plus difficile.

Le nombre **d'un millions de logiciels malveillants** a été dépassé en 2008
Plus de **3200 nouveaux virus** ou variantes font leur apparition chaque mois.
(F-Secure 2008)

Nombre d'attaques virales lors du 1er semestre 2005 (Rapport IBM) :

- Agences gouvernementales : 50 millions
- Secteur industriel : 36 millions
- Secteur financier : 34 millions

Types de codes malicieux :

On peut citer divers types de codes malicieux :

- **Virus** : la propagation utilise la complicité involontaire de la victime (e-mail, pop-up).
- **Vers :** la propagation est autonome via réseau (sans action d'un utilisateur).
- **Troyen** (cheval de Troie) qui dissimule son aspect nocif en prenant l'aspect extérieur d'un programme inoffensif ou attractif.
- **Backdoor** qui installe une porte dérobée, permettant à un attaquant de pénétrer dans un système.
- **Sniffers,** système d'écoute des communications réseau.
- **Keyloggers,** système enregistreur (logiciel ou matériel) des touches clavier.
- **Bombes logiques** qui se déclenchent sur évènement particulier (anniversaire).
- **Virus macro** : utilisation des possibilités de scripts applicatifs (Word, Excel, …).
- **RootKit** qui permet de maintenir la présence d'un code malicieux sur un système compromis par l'utilisation de techniques de furtivité (cacher des processus, fichiers, clef de registre, …).
- **Hoax** qui est un canular avec pour objectif l'engorgement ou la désinformation.

Si auparavant l'objectif des créateurs de codes malicieux était de relever des défis techniques, de semer le trouble, désormais leur motivation est tout autre. Le but est de « gagner de l'argent ». Les botnets (réseaux de robots) en sont de bons exemples. Après avoir contaminé des milliers ou centaines de milliers d'ordinateurs (bots), l'attaquant (le gardien des bots ou botmaster) peut en prendre le contrôle sans que leur propriétaire s'en aperçoive. On dit que ces ordinateurs sont alors des zombies.

Ainsi, l'attaquant utilise cette armée de zombies, véritable « force de frappe » pour :

- saturer des sites web (déni de service) en concentrant des milliers de sollicitations simultanées.
- envoyer des millions de courriers de type SPAM, phishing.
- fouiller et dérober le contenu des ordinateurs zombies.

On assiste donc à

- du « cyber racket » : des sites Internet ont été rendus inaccessibles pendant plusieurs jours car ils avaient refusé de payer une rançon.
- la location de Botnet pour l'envoie de spam, pour procéder à des denis de service du site de concurrents ou à de l'espionnage industriel, …
- et même des guerres entre gangs maitrisant des Botnets !

En aout 2008, les autorités néerlandaises ont arrêté un botmaster de 19 ans qui était à la tête du botnet Shadow contrôlant plus de 100 000 machines zombies.

Espiogiciel ou spyware :

Les spywares sont des programmes chargés de recueillir des informations sur l'utilisateur de l'ordinateur sur lequel ils sont installés. On trouve trois types de spywares :

- Commerciaux : Profilage des internautes (saisie des URL, Mots-clés,…).
- Affichage de bannières publicitaires.
- Mouchard : Récupération de données personnelles.

L'installation des spywares s'effectue généralement en même temps que d'autres logiciels (freewares, sharewares,…). D'ailleurs cette installation n'est pas forcément illégale car elle est stipulée dans conditions d'utilisation des logiciels que l'on « accepte » après les avoir lu consciencieusement ! Mais les spywares peuvent être illégaux selon la nature des informations « trackées ».

33% de tous les disfonctionnements des applications Windows, sont causé par des spywares. (MS Watson/OCA, 2004)

Protection et Prévention

La protection contre les codes malicieux passe par la mise en place de suites de sécurité intégrant antivirus, antispyware, antirootkit, parefeu personnel (pour surveiller les échanges entre l'ordinateur et l'extérieur). Pour contrer l'évolution permanente des codes malicieux, il est vital de souscrire aux mises à jour « temps réel » de ces suites de sécurité.

Il faut néanmoins être conscient, que cela ne constitue pas une protection infaillible. Etre vigilant avec les sites que l'on consulte, le contenu des e-mails que l'on ouvre, les logiciels que l'on installe, les supports d'échange que l'on utilise (clé usb, …), constitue un premier niveau de prévention

Vulnérabilité et Intrusion : le vol à l'étalage

Une intrusion dans le système d'information correspond à l'accès non autorisé à une ressource logique. Par exemple, pénétrer dans un réseau d'entreprise ou un réseau wifi, parcourir et accéder aux données d'un ordinateur, d'un serveur.
Cette notion d'autorisation est définie par le responsable du SI et s'entend sur tout ou partie du système d'information (un employé peut être autorisé à accéder à certaines fonctions du SI et pas à d'autres).
Ce n'est pas parce que le SI n'est pas, ou mal protégé, que cela confère un droit ou une excuse d'intrusion. Néanmoins, un SI mal protégé est sujet à des tentatives et tentations d'intrusions.

Un ordinateur non protégé, connecté à internet subit en moyenne **100 attaques par jour.**

Les procédés sont divers : profiter des vulnérabilités ou des failles d'un système ou d'une application, de mauvais paramétrages, utiliser des codes malicieux, utiliser l'ingénierie sociale pour la récupération de mots de passe, ...

Les intrusions ont des objectifs multiples pour leur auteur : Utiliser le SI pour des attaques par rebond (utilisation d'un SI tiers piraté pour attaquer la cible voulue), Défiguration de site Web, Altérations ou vols de données (en forte croissance).
Tous les systèmes sont concernés : Ordinateurs, téléphones portables, consoles de jeux, éléments réseaux, Les intrusion touchent aussi bien les couches matérielles que Réseau, Systèmes ou Application.

Du point de vue juridique, en France, le Délit d'intrusion est punit par le code pénal (L.323-1) de 1 an de prison et 15 000 € d'amende. Cette peine est multipliée par trois (3 ans de prison + 45 000 €) en cas d'altération, suppression de données (L.323-3).

Protection et prévention

Les éléments de prévention et protection en matière d'intrusions, sont :

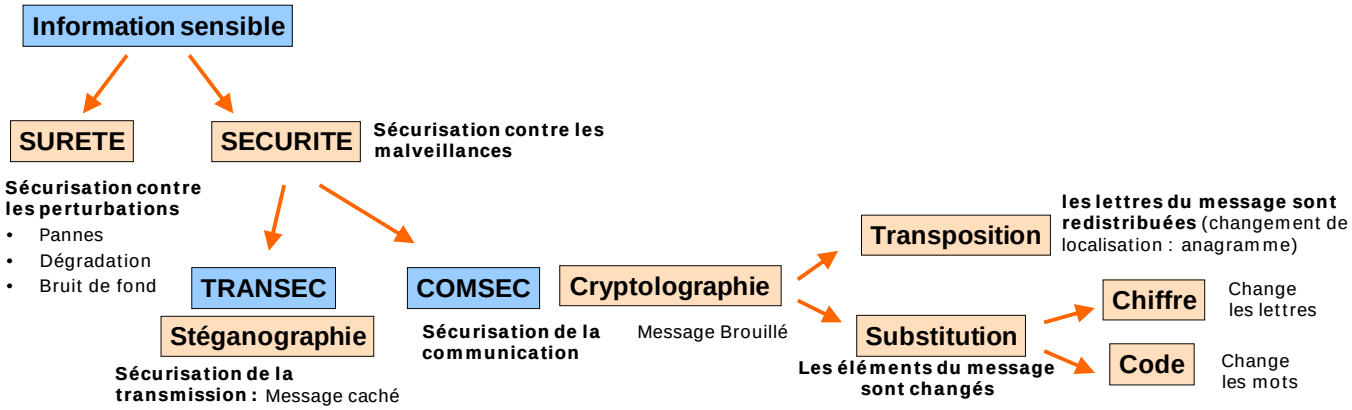
- Restriction des accès (logiques et physiques), Paramétrage limitatif.
- Identification des utilisateurs (mot de passe, certificat électronique, biométie,…).
- Filtrage et validation des échanges : Firewall.
- Infrastructure réseau compartimentée (pour limiter la propagation).
- Protection des réseaux sans fil (activation des systèmes de sécurisation basique, liste d'approbation ou refus des ressources, isolation du réseau sans fil, …).
- Mise à jour des systèmes (logiciel et matériel) contre les failles et vulnérabilités.
- Systèmes de détection :
    - IDS / IPS : Détection automatique d'intrusions via analyse des échanges
    - Pot de miel/ Honeypot : attirer les intrus vers des leurres pour les identifier
    - Analyse des fichiers de trace (log)
    - Outil de détection de changement de contenu de site web

La protection de l'information

La protection de l'information est une des composantes majeures de la sécurité des systèmes d'Information dans la lutte contre la perte, l'altération des données (par malveillance ou autre) et le vol de l'information. On a deux types d'informations sensibles :

- L'information « Secret Défense » dont la protection est régie par la loi.
- L'information « Confidentielle » liée à des secrets ou à la discrétion professionnelle (en général régie contractuellement).

La protection de l'information est assurée par la sureté d'une part et la sécurité de l'information d'autre part.



La sureté de l'information

La sureté de l'information consiste à protéger la donnée contre les perturbations ne provenant pas d'actes de malveillance (les pannes, dégradations, bruit de fond lors d'échanges de données). Les solutions sont basées sur l'utilisation de modèles provenant de l'analyse de comportements statistiques. Par exemple

- La théorie des codes pour la détection et / ou la correction d'erreurs.
- La redondance de systèmes : Fail Over, Load Balancing, Stockage RAID.

La sécurité de l'information

La sécurité de l'information consiste à protéger la donnée contre les actes de malveillance. L'objectif est d'assurer l'intégrité, l'authentification, la non répudiation et surtout la confidentialité de l'information.

Cet aspect a influencé l'histoire des peuples. C'est une exigence qui remonte à la nuit des temps, en réponse aux besoins d'échanger en toute discrétion pour les gouvernants, les militaires, les diplomates, les bandits ou les amants passionnés. On assiste depuis lors, à une « course poursuite » entre ceux qui élaborent les techniques de dissimulation et ceux qui tentent de les « briser », les cryptanalystes. En matière de sécurisation, deux procédés sont disponibles.

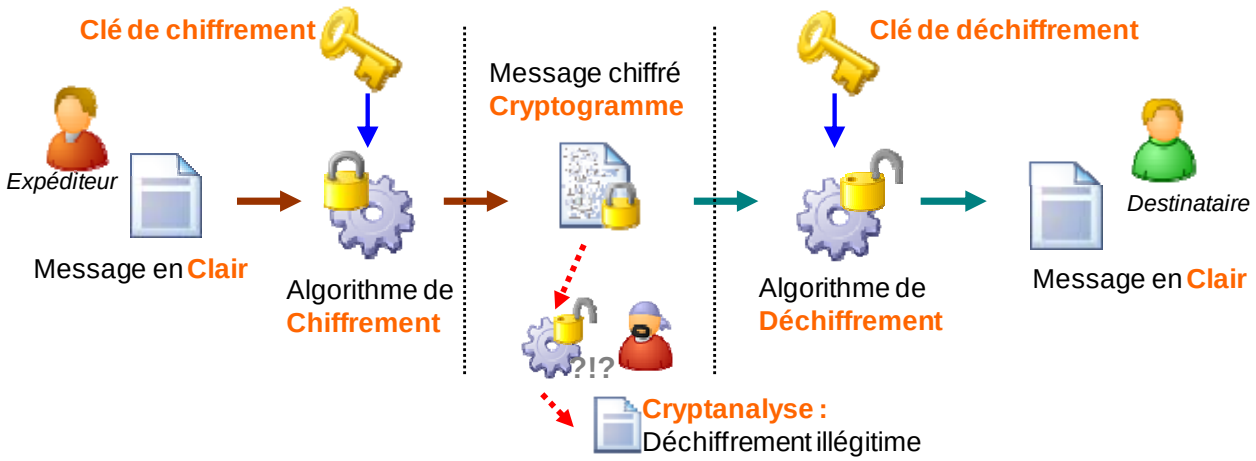
La sécurisation de la communication (COMSEC) : La donnée est transmise, mais incompréhensible. Mais on sait qu'une information (illisible) est communiquée; ce qui est en soit déjà une information : le cryptanalyste sait qu'il ne sait pas !

La sécurisation des transmissions (TRANSEC) : La donnée et la transmission de celle-ci sont dissimilées : le cryptanalyste ne sait pas qu'il ne sait pas. La technique utilisée est la **stéganographie** qui permet sur un support anodin dont l'échange ne déclenche pas de soupçon (fichier Image, Fichier Vidéo, Fichiers son, …) de dissimuler une information.

Chiffrement de César:

Il s'agit d'un des Chiffrements les plus anciens. Il était utilisé par Jules César. Le Principe : Substituer un caractère par un autre via un décalage des lettres de l'alphabet. Par exemple avec un décalage de 3 (la clé), « veni, vidi, vici » devient « YHQL, YLGL, YLFL ».

Pour le COMSEC, la technique utilisée est la **cryptologie,** permettant de crypter ou chiffrer des messages en les rendant incompréhensibles. L'action inverse, est le déchiffrement. On parlera de décryptage pour le déchiffrement illégitime.



Trois types d'algorithmes permettent de procéder à la cryptographie :

- **Chiffrement symétrique** : Une même clé (clé secrète) permet de chiffrer et déchiffrer (exemple chiffrement de César). Il s'agit en général de procédés fiables et rapides mais nécessitant un échange sécurisé de la clé.
- **Chiffrement asymétrique** : un couple de clé : publique et privée permet respectivement de chiffrer et déchiffrer (Exemple Algorithme RSA). Si ce procédé résout le problème d'échange de clé, il présente l'inconvénient d'être très lent.
- **Chiffrement hybride** : il s'agit d'un mixte des deux procédés précédant en combinant les avantages de chacun (exemple le SSL pour protéger les transactions financière sur Internet).

Aujourd'hui la cryptographie est un élément essentiel dans la sécurisation des Systèmes d'Information. Elle permet :

- La confidentialité des données sensibles qui sont stockées ou échangées.
- L'authentification des ressources (signature électronique, certificats numériques, …)
- L'intégrité et la non-répudiation des transactions.

Les aspects juridiques

Les aspects légaux et règlementaires ne doivent pas être négligés dans le cadre de la sécurité des systèmes d'information. Certes, il est nécessaire pour les organismes de s'y conformer pour éviter les risques de poursuites judiciaires mais il faut aussi s'y appuyer comme un élément de protection complémentaire. La lutte contre la cybercriminalité passe par la sollicitation des forces de l'ordre et des autorités judicaires qui se sont fortement adaptés dans ce domaine ces dernières années. Voici quelques éléments à considérer :

Intrusions dans un SI : voir chapitre « Les vulnérabilités et intrusions : le vol à l'étalage »

Loi encadrant les e-mailing commerciaux
En France, la loi pour la confiance dans l'économie numérique (LCEN) du 21 juin 2004 encadre l'utilisation du e-mailling dans le cadre des emails non désirés.

Propriété intellectuelle (loi du 11 mars 1957)
L'utilisation d'une œuvre de l'esprit (littéraire, musical, artistique, logiciel). sans consentement de son auteur relève de la contrefaçon (300 K€ + 3 ans de prison).

Libertés individuelles (loi du 6 janvier 1978)
Toute collecte et stockage d'information à caractère personnel est réglementé avec une déclaration à la CNIL. L'informatique ne doit pas porter atteinte à l'identité humaine, aux droits de l'homme, aux libertés individuelles et publiques et à la vie privée.

Contenus illicites
La diffusion de contenu (sur les réseaux de communication) engage la responsabilité des éditeurs et dans certaines conditions les fournisseurs d'accès et hébergeurs vis-à-vis de :

- L'atteinte à la vie privée, La diffamation.
- L'apologie et la provocation aux crimes et délits,
- L'incitation à la discrimination, au suicide, à la haine raciale, à la violence, …
- Le Racisme, la Pédophilie, …
- La Contrefaçon (propriété intellectuelle)

La consultation de certains contenus (par exemple la pédophilie) est passible de poursuites, notamment pour l'organisme si la consultation provient de son Système d'Information.

Sanctions Pénales *(Exemples):*

Falsification de document informatique :
45 K€ + 3 ans de prison

Fraude monétique (via informatique) : de 450 à 750 K€ + 1 à 7 ans de prison

Recel de données (provenant d'un délit) :
350 K€ + 5 ans de prison

Escroquerie, usurpation d'identité : de 350 à 750 K€ + de 5 à 7 ans de prison

Vol de données :
45 K€ + de 3 ans de prison

Atteintes aux secret des correspondances :
45 K€ + de 1 an de prison

Intrusion dans un SI :
15 K€ + de 1 an de prison

En cas d'infraction ou de « cyber agression », il ne faut pas hésiter à porter plainte en mettant en produisant des éléments techniques fiables qui aideront les autorités dans leur enquête. Dans la stratégie de sécurisation, être en mesure de collecter des « empreintes numériques », des preuves, est primordial. Il ne faut surtout pas procéder à ses propres contre-attaques, qui seraient juridiquement néfastes : Nul n'a le droit de se faire justice lui-même !

Concevoir des solutions sécurisées : Une nécessité

Infrastructures sécurisées

Aujourd'hui il existe de nombreuses solutions dans la protection et la prévention des infrastructures techniques. Elles doivent répondre à une stratégie définie, en intégrant les aspects suivants :

- Périmètre et Cloisonnement des réseaux.
- Gestion de l'authentification, Goulets d'étranglement.
- Gestion du moindre privilège.
- Confidentialité des flux.
- Détection, Traçabilité, Supervision.
- …

Parmi les solutions, on peut citer quelques exemples :

- Gestion de l'authentification (Login/mot de passe, Cartes à puce, Annuaires, Infrastructure à clés publiques, Biométrie,…).
- Protection des canaux de communication sensibles (VPN, Cryptage,…).
- Antivirus, Antispyware, Antirootkit, …
- Redondance des ressources critiques.
- Paramétrage restrictif systématique des Systèmes.
- Filtrage et Cloisonnement (Firewall, Proxy, Reverse Proxy, DMZ, NAT, …).
- Détection d'intrusion (IDS, IPS), Pot de miel (leurres).
- Journalisation (fichiers log), Monitoring des ressources.
- …

Applications et systèmes sécurisés

Concevoir des applications sécurisées, c'est-à-dire fiables et présentant une surface d'attaque minimale, devrait être une obsession pour les équipes de développement logiciel. Malheureusement, cela reste encore souvent qu'un vœu pieux ! Si la notion de sécurité est assez bien établi dans l'exploitation informatique, cela est encore rare dans la conception logicielle même chez de grandes SSII ou éditeurs de logiciels reconnus.

70 % des attaques des sites web exploitent des failles de la couche applicative et non des couches système ou réseau.

Alors que la sécurité devrait être une fonctionnalité à part entière, elle est souvent négligée face aux contraintes de délais et aux exigences fonctionnelles des clients. Il faut reconnaitre que des efforts considérables ont été réalisés dans l'approche qualité logicielle (grâce aux normes et méthodologies), mais le volet sécurité est encore le parent pauvre. Pourtant, une application non sécurisée coûte cher (correctif, image de marque, perte

d'exploitation, …). Je suis navré de constater encore le peu de formations dispensées sur l'approche sécurité applicative aux futurs concepteurs de logiciels.

Les failles ou vulnérabilités applicatives que l'on rencontre sont principalement :

- **Buffer Overflow** : Exécution de code 'pirate' par une application en lui envoyant un volume de données supérieur à celui attendu causant une modification du flux d'exécution.
- **Cross Site Scripting** (XSS) Insertion par l'attaquant de code HTML ou java script dans une page web fourni par un serveur. Ce code est exécuté dans le navigateur client.
- **SQL Injection**: Insertion par l'attaquant de commandes SQL via des entrées applicatives pour modifier une instruction SQL exécutée dans l'application.
- **Déni de Service** : Saturation d'une ressource (matérielle, logicielle, réseau,…).

Ces failles, exploitent les points faibles négligés par les équipes de développement :

- la confiance injustifiée dans les entrées (validations inefficace ou inexistante).
- le manque de protection des données (stockage ou échange en clair).
- les problèmes de configurations (gestion des privilèges).
- le traitement des cas improbables.

La sécurisation des applications doit intervenir durant toutes les phases d'un projet, depuis des spécifications jusqu'à la recette. Durant la phase de conception il faut procéder à une analyse sécuritaire pour réduire les potentialités de failles ou vulnérabilités.

En termes de bonnes pratiques de la sécurité applicative citons les essentielles :

- **Contrôle systématique des codes de retour** pour prévoir l'échec, l'improbable et échouer en mode sécurisé.
- **Contrôle et Validation de toutes les entrées.**
- Exécution avec le **moins de privilèges** possibles.
- **Non stockage d'informations confidentielles en 'clair'**
- Non affichage de messages trop explicites (qui aideraient de potentiels pirates).
- Contrôle des capacités des ressources avant les traitements complexes.
- Interception et traitement des exceptions.
- Gestion du transactionnel.

Pour illustrer ces propos, je vais m'attarder sur une expérience révélatrice qui m'est arrivée lors de l'un de mes cours sur la sécurité applicative. Cet exemple fut un cas « fabuleux » en terme pédagogique.

Lorsque vous présentez à des étudiants, les différentes techniques d'attaques d'un site Internet, il ne faut pas attendre très longtemps pour les voir mettre en application ce que vous leur montrez. Effectivement, il y a quelques années, un étudiant a voulu « évaluer la résistance » d'un intranet d'une faculté (dont je tairai le nom) à de l'injection SQL. Après m'en avoir informé, cet étudiant a présenté à l'ensemble de la classe, son « exploit ». Outre la vulnérabilité sur l'injection SQL, cette technique lui a permis de pénétrer dans l'espace restreint du site avec les droits Administrateur. Ce statut donnait la possibilité d'accéder à la totalité des listes d'élèves avec toutes leurs coordonnées, et pire, leur mot de passe d'accès en clair. Comme la plupart des individus utilisent le même mot de passe, il a été facile en prenant un utilisateur au hasard (son email et son mot de passe), d'accéder au webmail de son opérateur internet, et de visualiser la liste d'emails de cet utilisateur malheureux. Une analyse très succincte a mis en évidence que cet utilisateur avait un compte sur un célèbre site de vente aux enchères. Sans faire le test, il était fort à parier que son accès à ce site était protégé par le même mot de passe. On aurait donc pu faire quelques achats sur le compte de cet infortuné élève !

Cet exemple est l'illustration parfaite de trois graves fautes de conception en matière de sécurité d'une application logicielle (en l'occurrence l'intranet) :

- vulnérabilité à l'injection SQL.
- échec en mode non sécurisé (hériter du statut administrateur lors d'une carence d'identification, due à l'intrusion).
- stockage et affichage des mots de passe des utilisateurs en clair.

Ces trois fautes, mettaient en défaut la sécurité des informations privées sur les élèves de cette faculté et leur patrimoine. On imagine aussi, que des élèves « hacker » auraient pu changer à leur convenance les notes de partiels ! Pour la petite histoire, après avoir mis en garde mon étudiant qu'il était passible du délit d'intrusion, il a signalé au webmaster du site les failles découvertes. Il s'est vu proposé un stage pour sécuriser le site intranet !

Système d'Information sécurisé

Sécuriser un système d'information, c'est mettre en œuvre ce que l'on vient de présenter (les infrastructures et les applications), mais c'est aussi :

- La mise en place d'une politique de sauvegarde.
- La gestion des aspects humains (cf. § L'homme : le maillon faible).
- La protection de l'environnement physique (verrouillage et surveillance des locaux, détection incendie, protection contre le vol, redondance électrique, …).
- Le Plan de reprise et de continuation, qui défini la mobilisation et les actions à faire en cas d'incidents ou de sinistres, pour garantir au SI une continuation d'activité (même dégradée) et assurer un retour à la normale rapidement.
- …

Bref il s'agit là de la politique de sécurité du SI. Pour être efficace, l'élaboration de cette politique et son suivi doit suivre une démarche : le management de la sécurité.

Management de la sécurité : une vision globale

Le Management de la sécurité consiste à mettre en œuvre et appliquer une politique de Sécurité du SI globale et cohérente et adapté à l'organisme. Son application permet de :

- faire tendre vers zéro les risques engendrés ou subis par le Système d'information.
- limiter la perte d'exploitation.
- réduire les risques de pénalités et sanctions pénales.
- préserver l'image de marque et la confiance des clients, partenaires,…
- focaliser les ressources internes sur le cœur de métier de l'entreprise.

Ce processus de management de la sécurité de l'information a un prix. Le prix de la sécurisation est fonction de l'acceptance du coût du sinistre potentiel. Pour évaluer ce coût, il faut prendre en considération une multitude de paramètres dont certains peuvent s'avérer difficilement évaluables :

Coût de la sécurisation :

- Coût des systèmes de protection et de prévention.
- Coût lié à la charge de travail pour la mise en œuvre et le suivi de la sécurisation.
- Coût des assurances.
- Coût de la complexité induite des infrastructures.
- Coût lié aux contraintes subies par les utilisateurs.

Seulement **55 % des entreprises** sont dotées d'une Politique de sécurité de l'information (PSI).

31% des responsables sont incapables d'identifier les budgets consacrés à la sécurité" (Clusif 2008)

Coût du sinistre :

- Coût des dégradations matérielles et immatérielles.
- Coût d'investigation (honoraires d'experts, diagnostic, …).
- Cout de perte d'exploitation.
- Coût de réparation, récupération et reprise.
- Coût des pénalités et sanctions pénales.
- Coût de dégradation de l'image et perte de confiance.

Pour aider à optimiser l'investissement de la sécurisation, il faut se rappeler que l'on a une bonne protection si les moyens d'attaque sont supérieurs au gain que pourrait en tirer l'assaillant. Il n'est donc pas forcement nécessaire de surdimensionner la sécurité, au risque de dégrader la productivité de l'organisme. Il ne faut pas oublier le fameux adage « trop de sécurité tue la sécurité ». L'enjeu majeur en termes de management de la sécurité est donc d'identifier les priorités et de trouver le bon équilibre.

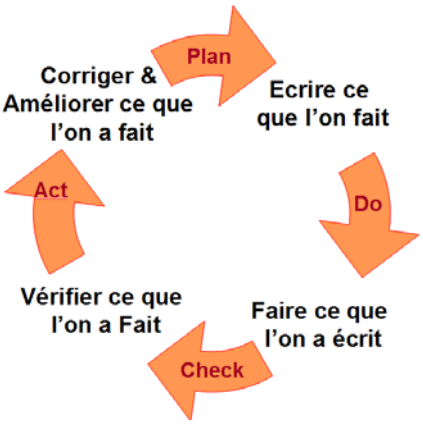
Normes et Méthodes

Des repères et référentiels sont disponibles pour aider à bâtir la politique de sécurité du SI. Les deux principales normes sont :

ISO 17799 : c'est la plus utilisée en matière de sécurité informatique, elle définit les objectifs et recommandations concernant la Sécurité de l'Information. Il s'agit en fait d'un référentiel pour élaborer une politique de sécurité, une analyse de risque, un audit, …

Famille ISO 27000 : Cette famille propose des normes certifiantes, des normes de recommandations et des normes sectorielles. En résumé, elle définit les exigences auxquelles doit répondre un SMSI (Système de Management de la Sécurité de l'Information). Elle repose sur la roue de Deming dit cycle PDCA (Plan, Do, Check, Act) avec un ensemble d'éléments itératifs permettant à un organisme :

- d'établir les objectifs et la politique de sécurité.
- d'appliquer cette politique.
- de contrôler l'atteinte des objectifs.
- d'améliorer la politique de sécurité.



D'autre part, il existe plusieurs méthodes (EBIOS, CRAMM, MEHARI, OCTAVE, CALLIO, COBRA,…) pour guider l'analyse de risque, la mise en place de politique de sécurité ou d'audit, en cohérence avec les normes citées ci-dessus.

L'analyse de risque

L'analyse de risque est un processus préalable indispensable pour établir une politique de sécurité ou procéder à un audit. Il permet **d'évaluer les risques par rapport au contexte de l'entreprise**.
Ainsi, à partir de cette analyse, la mise en place d'une politique de sécurité, sera de minimiser, c'est à dire rendre acceptable les différents risques pour l'entreprise. En synthèse la méthodologie consiste à évaluer pour chaque risque (lié à une menace et un mode opératoire) :

- **La potentialité**, c'est-à-dire la probabilité de l'occurrence que le risque survienne en tenant compte du contexte de l'organisme et des mesures de sécurité en place (localisation, activité, enjeux commerciaux, équipements, solutions de préventions, de protection, organisation, compétences humaines, ennemis potentiels,…).
- **L'impact**, c'est-à-dire la gravité des conséquences directes et indirectes, si le risque se produisait en tenant compte des confinements, des palliatifs ou des transferts du risque qui pourrait réduire les conséquences (sauvegardes, plans de reprise d'activité, assurances, …).

« Le seul système informatique qui est vraiment sûr est un système éteint et débranché, enfermé dans un blockhaus sous terre, entouré par des gaz mortels et des gardiens hautement payés et armés. Même dans ces conditions, je ne parierais pas ma vie dessus. »
Gene Spafford, fondateur et directeur du Computer Operations, Audit and Security Technology Laboratory.

L'audit Sécurité

L'audit consiste à analyser et à évaluer la définition et la mise en application de sécurité du SI sur un périmètre donné (Entreprise, Direction, Service, …). Il s'agit d'un Constat à un instant T qui va **évaluer les services de sécurité** en termes d'**efficacité** (capacité à assurer sa fonction), de **robustesse** (capacité à résister à une action d'inhibition) et de **mise sous contrôle** (capacité et rapidité de détection de son dysfonctionnement et les moyens de réaction).

Plan Stratégique de Sécurité du SI définit la politique de Sécurité

Le PSSI consiste à élaborer et décrire le processus de mise en œuvre de la sécurisation du système d'information en fonction de contexte et l'environnement de l'entreprise. Il s'agit d'un processus itératif et continu face aux évolutions de l'organisme d'une part et des menaces et modes opératoires d'autre part. Quelque soit l'organisme, ce processus est très important. Il ne doit pas être géré au jour le jour, au gré des incidents, sans vision globale. Le plan stratégique de sécurité du SI doit :

- être sous la responsabilité d'un interlocuteur clairement identifié ;
- formalisé sous forme de document et à jour ;
- validé par la Direction Générale ;
- classé confidentiel au sein de l'organisme.

L'approche consiste à élaborer un SMSI (norme 27001), en répondant à un questionnement usuel. La démarche itérative est la suivante :

- Quoi Protéger et Pourquoi ? : Inventaire des actifs numériques, et Infrastructures
- De Quoi les protéger ? : Inventaire des menaces et des modes opératoires
- Quels sont les Risques ? : Analyse des risques (potentialités, impacts)
- Comment Protéger ?

- Organisation, Méthodologie et Procédures.
- Politique de sauvegarde.
- Protection et prévention des aspects humains.
- Protection et prévention des ressources logiques.
- Protection et prévention de l'environnement physique.
- Surveillances et Contrôles, La Veille et Audit.
- Plan de reprise et de continuation.

Sans être exhaustif, on peut synthétiser les actions de protection et prévention d'un organisme sur le schéma ci-dessous.

De la Protection à la Maitrise Stratégique de l'Information

La guerre de l'information

Comme nous l'avons évoqué en début de ce livre blanc, l'espace informationnel s'ajoute aux espaces terrestres, maritimes et aériens, nécessitant un ajustement tactique et sécuritaire. Cela entre naturellement dans le champ des compétences régaliennes des Etats. L'objectif de la guerre de l'information, de la « cyber guerre », du « cyber terrorisme », est de paralyser l'économie, l'administration ou le quotidien des citoyens. La difficulté de défense réside dans les caractéristiques de ces « guerres » liées à la géopolitique : assaillants multiples aux divers profils, contours des menaces flous, champs de bataille élargies, délais de réaction réduits, attaque en temps de paix, … Ainsi, suite à des attaques de "cyber guerre" l'OTAN a décidé de créer son premier centre de formation pour la cyber défense". Aujourd'hui, l'ensemble des nations intègre cette dimension et procède ainsi à l'adaptation de leurs armées et leur défense nationale.

Avril 2007, **cyber affrontement** entre russes et estoniens suite à l'enlèvement à Tallin d'un mémorial de soldats soviétiques. Rapidement, l'Estonie, a subi une série d'attaques importantes (déni de service, virus). Les cibles: sites gouvernementaux, banques, médias et organisation politiques. Même les appels aux urgences (ambulances, incendies) sont restés indisponibles pendant plus d'une heure.

La dimension défensive et offensive.

Au niveau des Organismes et des Entreprises, manager la sécurité, c'est donc prendre en compte (entre autres) la protection de l'information, car l'information est une cible, un objectif pour les « agresseurs ». Si l'on veut rentrer dans un processus d'amélioration et mieux, raisonner en termes d'efficacité et d'investissement, il devient opportun de considérer **l'information aussi comme une arme**, et de s'en servir en conséquence. On parlera alors de maitrise stratégique de l'information, où en parallèle de l'aspect purement défensif, on s'intéressera aussi à l'aspect offensif.

Pour cela, au delà des référentiels, des bonnes pratiques, il est important de faire preuve d'adaptabilité, de raisonnement stratégique, de remettre parfois en cause des usages et des conventions, bref de **faire appel à l'intelligence**.

Ainsi, la dimension sécuritaire doit trouver une consolidation et un prolongement naturel vers l'intelligence économique.

L'intelligence économique : S'informer pour décider et agir

L'Intelligence Economique est l'ensemble des actions de recherche, de traitement et de diffusion (en vue de son exploitation) de l'information utile aux acteurs économiques, pour améliorer la compétitivité et mieux se protéger. L'utilisation stratégique de l'information est au cœur de l'Intelligence Economique: **La bonne information, au bon moment, à la bonne personne**. L'information doit être obtenue légalement (éthique des affaires) et alimenter un processus de collecte et d'analyse basé sur l'intelligence collective, en prenant en compte la sous-information, la sur-information, la désinformation.

Le RSSI : une compétence transverse, un rôle stratégique

Le Responsable de la Sécurité du Système d'information (RSSI), est la clé de voute de la Politique de Sécurité. Il est à la fois l'Auteur et le Chef d'Orchestre de la Sécurisation.

Parfois je rencontre des responsables, qui fièrement me soutiennent haut et fort que leur SI est fiable et sécurisé à 100%. Leur SI ne présente « aucune faille, aucune ! »
En fait, ce qu'ils ignorent, c'est que leur SI présente bel et bien une faille de sécurité, une faille qui n'est autre qu'eux même. Ce genre de certitude est une faille en soit, car la principale qualité d'un responsable sécurité est la remise en question permanente.

Le garant de la politique de sécurité

Le RSSI endosse la responsabilité de la sécurité du SI et de la protection de l'information de son organisme. Idéalement, il doit être rattaché à la Direction Générale, ce qui lui donne une légitimité (nécessaire) et lui confère un rôle transversal et global pour une cohérence d'ensemble. Il peut être à la tête d'une équipe dédiée (Ingénieurs, consultants sécurité) ou de correspondants « sécurité » dans chaque département de l'organisme.
Le RSSI définit et met en œuvre la politique de sécurisation du SI. Il supervise et contrôle son application. Il assure également son évolution et son amélioration.

Le Rôle du Responsable de la Sécurité du Système d'information va dépendre de l'organisme et de la maturité de celle-ci vis-à-vis de la maitrise de l'information. Ainsi, graduellement son périmètre de compétence est positionné sur :

1. Une approche purement technique.
2. Le développement d'une politique sécurité de l'information.
3. La propagation d'une culture sécurité : diffuser le Savoir Faire et Faire Savoir.
4. La participation à la stratégie de la maitrise de l'information.

Néanmoins, le rôle du RSSI peut être frustrant et parfois ingrat, car en cas d'incident ou de sinistre sa responsabilité sera systématiquement engagée. Mais quand tout fonctionnera sans aucun problème, se posera alors la question de son utilité (pourquoi dépenser des budgets lorsque tout va bien !). Autrement dit, il faut pouvoir démontrer en permanence, la pertinence et l'efficience de la politique de sécurité et la maitrise de l'information de l'organisme, notamment à travers des indicateurs, des tableaux de bords et de la veille.

La multi-Compétence

Comme nous l'avons vu, la sécurisation des SI est un vaste domaine, qui fait appel à de nombreuses qualités. Ainsi, on attend du RSSI de multiples compétences en termes de :

- Sécurité : Management du risque.
- Technique : Réseau, Système SI, architecture technique et applicative.
- Managériale : encadrement, gestion de projet; conduite du changement.
- Juridique : législation, réglementation, normes.
- Relationnelle : communication interne, externe, pédagogie.
- Stratégique : enjeux décisionnels, Qualité, Stratégie informationnelle.

Conclusion : « La Sécurité, c'est l'affaire de tous ! »

La sécurité est un des **fondements de la gouvernance des systèmes d'information**. La Sécurisation du système d'information est un processus itératif en quatre phases :

- La **Planification** en s'appuyant sur des normes et méthodes, en définissant les objectifs de sécurité en adéquation avec le métier et en procédant à une analyse de risques.
- La **Mise en œuvre** en élaborant un Plan Stratégique de sécurisation des SI, en intégrant la sécurité dans la gestion des projets, en développant des applications sécurisées et en maitrisant l'information stratégique.
- Le **Contrôle** avec la supervision, le monitoring et la vérification à l'aide d'audits de sécurité et de tests d'intrusions.
- L'**Amélioration continue.**

Comme nous l'avons vu, la sécurité des systèmes d'information doit reposer sur un responsable et son équipe. Ils doivent être polyvalents avec une vision stratégique en concordance avec le dispositif métier de l'organisme. Mais la sécurité sera efficiente si tous les acteurs de l'organisme sont conscients des risques et adaptent leurs comportements et leurs savoir-faire avec un leitmotiv « Protection de l'information ». En fait, au sein des organismes, la sécurité du système d'information est **l'affaire de tous**.

Pour terminer à la manière des dix commandements, j'évoquerai les attitudes qui me paraissent indispensables pour bien gérer la sécurité d'un Système d'Information :

1. Du temps pour la sécurité, tu dégageras.
2. Sur une démarche et une organisation structurée, tu t'appuieras.
3. Comme dernier rempart, la sécurité tu concevras.
4. Sans complexifier le processus métier, la sécurité tu aligneras.
5. Ni dans la paranoïa ni dans l'angélisme, tu tomberas.
6. Le mode de pensée de l'attaquant, tu adopteras.
7. Malgré la confiance, le contrôle tu n'oublieras pas.
8. Humble tu resteras mais déterminé tu seras.
9. De tes erreurs et de celles des autres, tu apprendras.
10. L'inévitable tu refuseras, l'inattendu tu envisageras.

En conclusion, à travers ce tour d'horizon synthétique, le processus de sécurisation du système d'information ne s'improvise pas. Il repose d'abord sur une **prise de conscience des hauts responsables** des sociétés et organismes, et sur la **sensibilisation de l'ensemble des acteurs**. Ce processus doit être confié et managé par des individus avec de réelles **compétences multi disciplinaires** et une **vision d'ensemble** de l'organisme et de son environnement. Les facteurs de réussites passent par la formation, la sensibilisation et la veille continue.

Les entités et les offres de formations du Groupe 4

Groupe 4 est un groupe de formation spécialisé dans le management de projet technique. Les formations "Sécurité" sont présentes dans les différentes entités :

1- **4IM et 4MM** : Dans le cadre des écoles en alternance Informatique-Management (4IMM) et Multimédia-Management (4MM), le management de la sécurité des SI est vu à travers des sessions dédiées de sensibilisation et d'approfondissement sur les 2 dernières années.

2- **Oplone *RAPID-Training*** : Dédié à la Formation Professionnelle Continue, Oplone propose des formules adaptées (sur catalogue ou sur-mesure) répondant aux besoins et attentes des donneurs d'ordres. Les formules RAPID-Training se déclinent sous forme de séminaires ou à travers un programme de formation de quelques jours (2 à 5 jours en inter-entreprises ou en intra-entreprise).

3- **Oplone *SMART-Training***: il s'agit d'un cursus de formation part-time de 3 jours par mois sur 10 mois (env 210 h) pour former des personnes en poste en entreprise voulant s'orienter ou se perfectionner dans le management de la sécurité des SI

4- **ISMP : Cursus CPTSSI** (Chef de projet Transverse en Sécurité des SI) : c'est un cursus long de niveau BAC +5, en 9 mois avec un stage de fin d'année. Il vise à former des experts et des managers en sécurité des Systèmes d'information, et amène aux métiers :
   - Ingénieur sécurité SI
   - Expert sécurité SI
   - Consultant sécurité SI
   - Responsable revue sécurité SI
   - Chef de projet Sécurité SI
   - Responsable Sécurité du SI

Le Groupe 4, c'est 100 % d'insertion professionnelle dès la fin de la formation

Sur la technopôle de Château-Gombert, à deux pas des calanques et des rivages méditerranéens, le Groupe 4 côtoient Centrale Marseille, Polytech Marseille, ainsi que les start up les plus innovantes du sud …

Les infrastructures du site – résidences et restaurants universitaires, piscine, installations sportives, Poste, parcs, métro, lignes de bus,… facilitent le quotidien sur place.

A quinze minutes du centre, Marseille, son centre ville et son Vieux-Port, offrent toutes les opportunités de loisirs, qu'ils soient sportifs, culturels, …

A trente minutes du centre, Aix en Provence met à votre disposition son activité nocturne.

RENSEIGNEMENTS :

Groupe 4
Bruno DOUCENDE
Technopole de Château Gombert
«Les Baronnies», Bat A
Rue Paul Langevin
13 013 - Marseille

Tel : 04.91.95.53.32
E-mail : bdoucende@groupe4.fr

www.groupe4.fr