Chapitre. I : GENERALITES sur La SECURITE des SYSTEMES INFORMATIQUES (Risques, Qualité, Audit et politique de Sécurité)

Les Objectifs du Cours :

- Permettre aux étudiants d'avoir une idée sur les enjeux et l'importance de la sécurité dans les systèmes d'information,
- Permettre aux étudiants de s'auto former sur les attaques et les grands principes de la sécurité informatique,
- Fournir aux étudiants, un ensemble d'outils de sécurité permettant de tester ou de sécuriser les réseaux et les systèmes,
- Consolider un ensemble de ressources liées à la sécurité d'un Système d'Information.

I. INTRODUCTION

Le progrès des technologies de l'information et de la communication au cours des dernières années a fait naître un grand nombre de systèmes d'information dans les organisations et administrations. Ces systèmes d'information, moteurs de croissance et de développement des métiers et services sont assez importants, voire même indispensables pour le bon fonctionnement de toute entreprise. Cependant, avec les menaces actuelles et les ouvertures des systèmes d'information sur l'Internet et d'autres réseaux non maîtrisés, Il devient nécessaire de garantir la sécurité de l'ensemble des biens constituant tout système d'information.

Assurer la sécurité d'un système d'information n'est plus un sujet tabou. Les statistiques des attaques et des menaces font qu'aujourd'hui, les responsables en sont conscients des risques pesant sur un système d'information, même si les moyens ne suivent pas toujours pour assurer effectivement et efficacement la sécurité.

II. GENERALITES SUR LES SYSTEMES INFORMATIQUES ET SUR LES SYSTEMES D'INFORMATION

A) Définitions d'un système informatique et d'un système d'information

1. Définition : Système informatique

Un système informatique est un ensemble de dispositifs (matériels et logiciels) associés, sur lesquels repose un système d'information. Il est constitué généralement des serveurs, routeurs, pare-feu, commutateurs, périphériques, médias (câbles, air, etc.), points d'accès, stations de travail, systèmes d'exploitation, applications, bases de données, etc.

2. Définition : Système d'information

Un système d'information est un ensemble de moyens (humains, matériels, logiciels, etc.) organisés permettant d'élaborer, de traiter, de stocker et/ou de diffuser de l'information grâce aux processus ou services. Un système d'information est généralement délimité par un périmètre pouvant comprendre des sites, des locaux, des acteurs (partenaires, clients, employés, etc.), des équipements, des processus, des services, des applications et des bases de données.

3. La sécurité d'un système

La sécurité d'un système (informatique ou d'information) est un ensemble de moyens techniques, organisationnels, juridiques et humains nécessaires et mis en place pour conserver, rétablir, et garantir

sa sécurité. En général, la sécurité d'un système d'information englobe celle du système informatique sur lequel il s'appuie.

REMARQUE

Faire de la sécurité sur un réseau consiste à s'assurer que celui qui modifie ou consulte des données du système en a l'autorisation et qu'il peut le faire.

B) L'évaluation de la sécurité d'un système informatique

L'évaluation de la sécurité d'un système informatique est un processus très complexe basé en général sur une méthodologie (standard ou non). Cette évaluation passe par une analyse de risques. L'analyse des risques pesant sur un système informatique elle-même s'appuie sur un ensemble de métriques définies au préalable.

On distingue généralement trois principaux critères de sécurité :

- **Disponibilité** : Elle consiste à garantir l'accès à un service ou à une ressource.
- **Intégrité** : Elle consiste à s'assurer que les données n'ont pas été altérées durant la communication (de manière fortuite ou intentionnelle).
- **Confidentialité** : Elle consiste à rendre l'information inintelligible à d'autres personnes que les seuls acteurs concernés.

En plus de ces trois critères, on peut ajouter les critères suivants :

- **Authentification** : Elle consiste à assurer l'identité d'un utilisateur, c'est-à-dire de garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être.
- **Non répudiation** : Elle consiste à garantie qu'aucun des correspondants ne pourra nier la transaction (en Envoi ou en Réception).

C) La Sécurité de l'information

Pour des soucis d'efficacité et de rentabilité, une entreprise communique aujourd'hui avec ses filiales, ses partenaires et va jusqu'à offrir des services aux particuliers, ce qui induit une ouverture massive à l'information. Par l'ouverture des réseaux, la sécurité devient un facteur décisif du bon fonctionnement de l'entreprise ou de l'organisme.

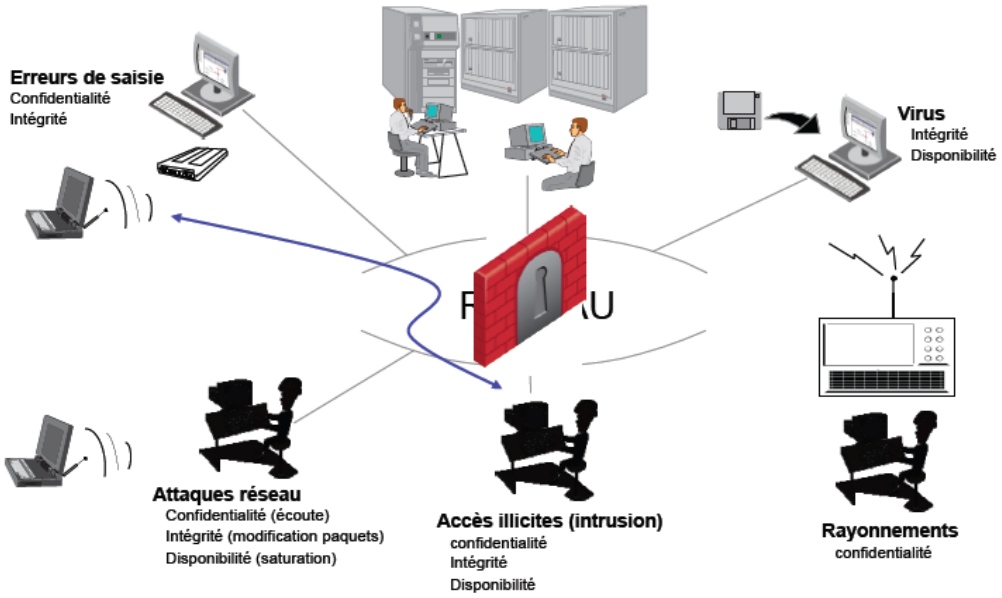
En fonction des enjeux, toute entreprise possède certaines informations qui ne doivent être divulguées qu'à un certain nombre de personnes ou qui ne doivent pas être altérées ou encore qui doivent être disponibles de manière transparente à l'utilisateur.

Ces informations feront l'objet d'une attaque si et seulement si des menaces existent et si le système abritant ces informations est vulnérable.

Par conséquent on appelle ***sécurité de l'information***, l'état de protection, face aux risques identifiés, qui résulte de l'ensemble des mesures générales et particulières prises pour assurer la confidentialité, l'intégrité et la disponibilité de l'information traitée, où :

- **la confidentialité** est le caractère réservé d'une information dont l'accès est limité aux seules personnes admises à la connaître pour les besoins du service.
- **l'intégrité** de l'information traitée garantit que celle-ci n'est modifiée que par un acte volontaire et légitime.
- **la disponibilité** est l'aptitude d'un système d'accéder à l'information dans des conditions définies d'horaires, de délais et de performances.

La sécurité des systèmes informatiques



D) Pourquoi protéger des informations ?

Parce qu'on estime que la perte des informations, cela provoquerait :

- **Une perte financière** (exemple : destruction de fichiers client, récupération de contrats par un concurrent,...),
- **Une perte de l'image de marque** (exemple : piratage d'une banque, divulgation d'un numéro de téléphone sur liste rouge,...),
- **Une perte d'efficacité ou de production** (exemple : rendre indisponible un serveur de fichiers sur lequel travaillent les collaborateurs).

D'où l'intérêt pour une entreprise ou un organisme d'avoir une classification de ses informations.
Par exemple, on peut citer les informations dites :

- ✓ **stratégiques** pour l'entreprise comme les offres de rachat en général ; ce sont des informations manipulées au niveau de la Direction de l'entreprise ou de l'organisme.
- ✓ **critiques** comme le plan d'adressage de l'entreprise, la configuration des outils de sécurité, les plans de secours,...
- ✓ **internes** comme l'ensemble des informations propres à l'entreprise et qui ne doit pas être forcément de notoriété publique,
- ✓ **publiques** comme les informations faisant l'objet de communiqué de presse ou les informations figurant sur le site Web de l'entreprise ou de l'organisme.

1. *Pourquoi y'a-t-il perte des informations ?*

Parce qu'une **menace** (une action ou un événement qui peut porter préjudice à la sécurité) s'est réalisée.

2. *Pourquoi cette menace s'est réalisée ?*

Parce que le système est **vulnérable**. Le système d'information comprend aussi bien le système informatique, le personnel...

3. *Pourquoi le système est-il vulnérable ?*

Parce que :

- Il n'existe pas de contrôle d'accès individuel aux applications,
- Il n'existe pas de système de sauvegarde,
- L'accès aux locaux est ouvert à tout public,
- Le personnel n'est pas sensibilisé à ce qu'il peut faire ou ne pas faire, dire ou ne pas dire.

III. La sécurisation des systèmes informatiques (enjeux, Menaces, Risques)

A) Les enjeux

On distingue généralement quatre principaux enjeux :

1. **Enjeux économiques :** La concurrence fait que des entreprises s'investissent de plus en plus dans la sécurisation de leurs systèmes d'information et dans la qualité de service fournit aux clients.
2. **Enjeux politiques :** La plupart des entreprises ou organisations se réfèrent aux documents officiels de sécurité élaborés et recommandés par l'État. Ces documents contiennent généralement des directives qui doivent être appliquées par toute structure engagée dans un processus de sécurisation du système d'information.
3. **Enjeux juridiques :** Dans tout système d'information, on retrouve de l'information multiforme (Numérique, papier, etc.). Le traitement de celle-ci doit se faire dans un cadre bien définit et dans le strict respect des lois en vigueur.

B) Les menaces

Les systèmes informatiques sont confrontés aux menaces. Une menace est un événement pouvant se produire à tout moment et que l'on craint. Selon leurs origines, les menaces peuvent être classifiées en deux catégories :

- Menaces d'origine naturelle (incendie, inondation, séismes, etc.)
- Menaces d'origine humaine (fuite, malveillance, espionnage, vol, etc.).

Elles peuvent, en s'appuyant sur la puissance de l'informatique, causer des dommages d'une ampleur inédite.

C) Les risques

Un risque est un événement susceptible de se produire.

Selon la nature physique, on peut classer les risques en plusieurs catégories dont voici quelques-unes : Accident, perte de services, vols, fuites d'information.

1) Risque "accident"

Cette catégorie regroupe tous les sinistres comme les incendies, dégâts des eaux, explosions, catastrophes naturelles, etc. Certains de ces risques ne peuvent être raisonnablement pris en compte (par exemple, un effondrement causé par la présence d'une ancienne carrière souterraine), d'autres peuvent être prévenus ou combattus (par exemple, un incendie), l'informatique n'étant alors qu'un des aspects du problème.

2) Risque "perte de services"

On range dans cette catégorie les coupures de courant, de télécommunications, les ruptures de stocks de fournitures essentielles, etc.

3) Risque "vol"

Ces problèmes sont la plupart du temps marginaux, sauf dans les grandes entreprises, l'administration et les établissements d'enseignement où les vols ou dégradations sont généralement commis par les personnes fréquentant habituellement les lieux (personnel, étudiants).

4) Risque "fuite d'informations"

IV. Les méthodes, les types d'attaques et les Outils.

A) Les méthodes et types d'attaques

Une « **attaque** » est une activité malveillante qui consiste à exploiter une faille d'un système informatique (serveurs, routeurs, système d'exploitation, logiciel, etc.) à des fins non connues par les responsables du système et généralement préjudiciables pour le système d'information en général.

Les attaques sont souvent menées suite aux motivations diverses :

- Perturbation du bon fonctionnement d'un système ou d'un service,
- Vol des informations sensibles (données bancaires par exemple),
- Utilisation des ressources du système à d'autres fins.

1. Attaque par intrusion

Ce type d'attaque vise à s'infiltrer physiquement ou logiquement dans un système informatique en vue de récupérer des informations exploitables à d'autres fins.

2. Attaque de l'homme du milieu (Man-In-The-Middle)

Ce type d'attaque vise à intercepter les communications entre deux parties (personne, ordinateur) sans que ni l'une, ni l'autre ne puisse s'en apercevoir. Il s'agit ici d'une attaque par interception. Le schéma ci-après illustre ce type d'attaque entre un ordinateur client et un ordinateur serveur.

3. Attaque par déni de service

Ce type d'attaque très fréquente, vise à perturber le bon fonctionnement d'un service. Elle exploite généralement les faiblesses de la pile de protocole TCP/IP et les vulnérabilités logicielles existantes et non traitées.

Par exemple, envoyer 1.000.000 de requêtes en moins de 5 secondes à un serveur web avec des adresses IP sources fictives, constitue une attaque de type déni de service sur le serveur Web.

4. Attaque par hameçonnage (phishing)

Le phishing est une technique dans laquelle des bandes organisées de cybercriminels se font passer pour des organismes financiers ou grandes sociétés en envoyant des emails ou des pages web frauduleux pour récupérer des mots de passe de comptes bancaires ou numéros de cartes de crédit pour détourner des fonds.

5. Attaque par dictionnaire et par force brute (mot de passe)

a) Attaque par dictionnaire

L'attaque par dictionnaire vise à retrouver un mot de passe à partir d'un dictionnaire élaboré au préalable. Elle consiste à tester une série de mots de passe potentiels, les uns à la suite des autres, en espérant que le mot de passe utilisé pour le chiffrement soit contenu dans le dictionnaire.

b) Attaque par force brute

L'attaque par force brute a le même objectif que l'attaque par dictionnaire, sauf que la technique change. Elle consiste à tester une à une, toutes les combinaisons possibles. Cette attaque est difficile d'aboutir lorsque le mot de passe contient plus de caractères variés (majuscules, minuscules, chiffres, caractère spéciaux).

1) Attaque par ingénierie sociale

Ce type d'attaque très fréquente également, vise à récupérer des informations sensibles des utilisateurs en s'appuyant sur leur naïveté. Elle exploite l'abus de confiance faite par les utilisateurs du système d'information.

Par exemple un hacker qui se fait passer pour un technicien du support en appelant une secrétaire pour lui demander le mot de passe d'ouverture de session sur son poste. Il s'agit là d'une usurpation d'identité.

B) Les outils d'attaque

Pour mener à bien les attaques sur les systèmes informatiques, les pirates utilisent des outils informatiques bien connus du domaine. Ces outils sont également utilisés par les administrateurs et spécialistes de la sécurité pour tester la robustesse de leurs systèmes d'information, généralement dans le cadre d'un audit de sécurité.

Parmi ces outils, nous pouvons citer :

- Les **programmes malveillants** (virus, ver, cheval de Troie, logiciel espion [spyware]),
- Les **scanners** et **sniffers,**
- Les **backdors** (portes dérobées),
- Les **spams** (courriers indésirables).

1. *Les programmes malveillants*

a) Définition : Virus

Un virus informatique est un programme malveillant conçu pour se propager à d'autres ordinateurs en s'insérant dans des programmes légitimes appelés « hôtes ». Il peut perturber plus ou moins gravement le fonctionnement de l'ordinateur infecté. Il peut se répandre à travers tout moyen d'échange de données numériques comme les réseaux informatiques et les CD/DVD, les clefs USB, etc.

b) Ver

Un ver informatique est un programme malveillant qui se reproduit sur plusieurs ordinateurs en utilisant un réseau informatique comme Internet.

Contrairement à un virus informatique, un ver n'a pas besoin d'un programme pour se reproduire. Il exploite les différentes ressources de l'ordinateur qui l'héberge pour assurer sa reproduction.

c) Cheval de troie

Un cheval de Troie est un programme d'apparence légitime conçu pour exécuter de façon cachée des actions à l'insu de l'utilisateur. En général, un cheval de Troie tente d'utiliser les droits appartenant à son environnement pour détourner, diffuser ou détruire des informations, ou encore pour ouvrir une porte dérobée qui permet à un attaquant de prendre, à distance, le contrôle de l'ordinateur.

d) Logiciel espion (spyware, mouchard ou espiogiciel)

Un logiciel espion est un programme malveillant qui s'installe dans un ordinateur dans le but de collecter et transférer des informations sur l'environnement dans lequel il s'est installé, très souvent sans que l'utilisateur en ait connaissance. Un logiciel espion est généralement composé de trois mécanismes distincts : Infection, collecte et transmission.

e) Rootkit

Un **rootkit** ("jeu de démarrage" en français) est un programme malveillant dont la principale fonctionnalité est de dissimuler la présence de son activité et celle des autres programmes néfastes aux yeux de l'utilisateur du système et des logiciels de sécurité (antivirus, pare-feu, IDS).

Certains rootkit peuvent en plus de cette fonctionnalité principale, installer des backdors (porte dérobée).

Les **rootkits** ont deux caractéristiques principales :

- Ils modifient profondément le fonctionnement du système d'exploitation,
- Ils se rendent invisibles (difficile à les détecter).

2. *Les sniffers*

Un sniffer est un outil matériel ou logiciel, permettant de lire les données qui circulent dans un réseau. Si les données sont non chiffrées, on peut obtenir des informations sensibles comme les mots de passe.

V. L'audit de sécurité

A) L'Audit, la conformité : référentiels de sécurité informatique

1. On considère un **audit de sécurité informatique** comme une mission d'évaluation de conformité par rapport à une politique de sécurité ou à défaut par rapport à un ensemble de règles de sécurité.

Une mission d'audit ne peut ainsi être réalisée que si l'on a défini auparavant un référentiel, c'est-à-dire en l'occurrence, un ensemble de règles organisationnelles, procédurales ou/et techniques de référence. Ce référentiel permet au cours de l'audit d'évaluer le niveau de sécurité réel de " terrain " par rapport à une cible.

2. Pour évaluer le niveau de conformité, ce référentiel doit être :

- **complet** (mesurer l'ensemble des caractéristiques : il ne doit pas s'arrêter au niveau système, réseau, télécoms ou applicatif, de manière exclusive, de même, il doit couvrir des points techniques et organisationnels) ;
- **homogène** : chaque caractéristique mesurée doit présenter un poids cohérent avec le tout ;
- **pragmatique** : c'est-à-dire, aisé à quantifier (qualifier) et à contrôler.

La mission d'audit consiste à mesurer le niveau d'application de ces règles sur le système d'information par rapport aux règles qui devraient être effectivement appliquées selon les processus édictés. L'audit est avant tout un constat.

Un audit peut être mené en suivant deux approches (non exclusives) :

- une approche " **boîte blanche** " : l'audit est alors déroulé in situ, les auditeurs ont accès à l'organisation, aux données et traitements réalisés, aux documents et processus appliqués. Ils font appels aux interlocuteurs autant que de besoin.
- une approche **" boîte noire** " : l'audit est alors mené en partant d'une connaissance limitée du système d'information cible. Les auditeurs opèrent sans accès a priori aux systèmes et données. Les " tests d'intrusion ou " tests intrusifs " font partie de cette catégorie d'audit.

Les deux approches précédentes sont complémentaires, en effet :

- Une approche " boîte blanche " est en général un audit plus homogène, l'évaluation possède une caractéristique d'analyse " en complétude " et les aspects techniques et organisationnels sont traités de manière uniforme ;
- Une approche " boîte noire " est en général un audit avec une vue plus parcellaire, révélant plutôt des lacunes ciblées à forte orientation technique.

Dans les deux cas, il est nécessaire de préserver l'opérationnel pendant les tests et validation technique de sécurité (qualité de service, performances, contraintes d'administration et de supervision).

B) Pourquoi réaliser un audit de sécurité?

Les objectifs d'un audit sont multiples :

- Une **validation des mesures de sécurité** mises en œuvre (contrôle, suivi qualité) ;
- Une **validation des processus** d'alertes, de réaction face à des sinistres ou des incidents : en déclenchant une simulation d'attaque logique ; ***par exemple***, on analyse la conformité de la réaction des acteurs avec les procédures en vigueur ;
- Une **détection** d'enjeux ou de lacunes "oubliées ";
- Une **sensibilisation** des utilisateurs, de la hiérarchie, des subordonnés aux risques encourus.

C) Les Limites d'un audit de sécurité

Parmi les limites dues aux démarches de certains audits, on cite :

- Les audits **"déclaratifs "**, c'est-à-dire dont les résultats reposent uniquement ou en grande majorité sur les déclarations lors d'entretiens avec les acteurs du système audité : cela introduit un biais du au contrôle volontaire/involontaire des audités sur les informations délivrées ;
- Les audits "techniques", c'est-à-dire dont la prise en compte des procédures et de l'organisation sont inexistantes (et parfois même sans adaptation au contexte) ;
- Les audits **"non techniques"**, c'est-à-dire dont la prise en compte directe (tests in situ) des configurations effectives des équipements systèmes, réseaux et applicatives n'est pas réalisée.

Les limites inhérentes des audits de sécurité sont par ailleurs les suivantes :

- Le temps imparti est restreint (la probabilité qu'une cause possible de futur incident de sécurité ne soit pas détectée n'est pas nulle) ;
- L'appréciation du contexte de l'entreprise (fonctionnelle, métier) est parfois délicate (un audit doit comporter ainsi une analyse minimale des enjeux et de la sensibilité des données et traitements) ;
- Le niveau de sécurité appliquée sur le système d'information est dynamique : il peut évoluer fortement en fonction d'une simple mise à jour de système d'exploitation ou d'applicatif par exemple.

Il est à noter qu'un résultat d'audit de sécurité peut être contredit par le moindre changement sur le système d'information (organisationnel ou technique).

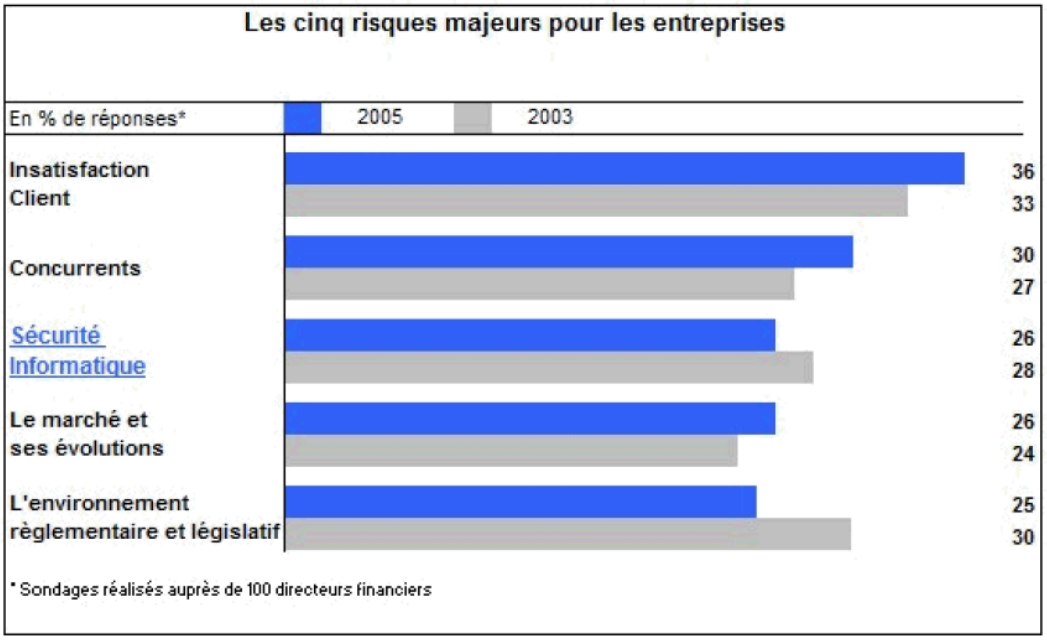
VI. La Qualité de la Sécurité.

A) La norme ISO 17799 : Le code de bonnes pratiques pour la gestion de la sécurité de l'Information

La **norme ISO 17799** est issue de la norme anglaise **BS7799** créée en 1995 et révisée en 1999. Cette norme constitue un code de bonnes pratiques pour la gestion de la sécurité de l'information.

La sécurité de l'information constitue l'un des domaines majeurs au sein des entreprises. Quel que soit le secteur concerné, Banque, Assurance, Recherche, Conseil, Informatique, etc.., L'omniprésence de l'informatique transforme la gestion de l'information en un processus stratégique.

Afin de garantir la disponibilité, la confidentialité ainsi que l'intégrité des données, l'entreprise doit réfléchir sur l'architecture de son système d'information, et mettre en place les moyens de surveillance et de parade adaptée. La pérennité de l'entreprise dépend du succès de la stratégie de sécurité définie.



(Source : Etude Risk Management 2005, TNS Sofres)

B) Principes de base de la norme

1. **Le modèle ISO 17799 : 2005**, par sa reconnaissance internationale et son exhaustivité de bonnes pratiques permettent à tout dirigeant d'améliorer le système de management de la sécurité de l'information de l'entreprise.

Par une analyse de risques approfondie et le choix d'actions ciblées, la société s'engage dans une démarche proactive visant à réduire les vulnérabilités et les risques majeurs détectés.

2. **L'ISO 17799 : 2006** fournit au Responsable du Système de Sécurité de l'Information (RSSI) la matière nécessaire à la bonne gestion de la sécurité au sein de l'entreprise. Quelques chapitres tels que l'analyse de risques, la définition de la PSI (Politique de Sécurité de l'Information) constituent les fondements essentiels à toute application.

3. **Les avantages de ce référentiel sont multiples :**

- Gérer les coûts de la sécurité (un management efficace assure un retour sur investissement rapide),
- Minimiser les risques économiques et civils encourus par l'entreprise,
- Développer une culture sécurité à l'ensemble des collaborateurs.
- Améliorer votre niveau de sécurité,
- Se mettre en conformité avec la réglementation.

4. **Rappel : la certification ISO**

La certification est le moyen d'attester, par l'intermédiaire d'un tiers certificateur, de l'aptitude d'un organisme à fournir un service, un produit ou un système conformes aux exigences des clients et aux exigences réglementaires.
C'est une Procédure par laquelle une tierce partie donne une assurance écrite qu'un produit, un processus, ou un service, est conforme aux exigences spécifiées dans un référentiel.

La famille des normes **ISO 9000** correspond à un ensemble de référentiels de bonnes pratiques de management en matière de qualité, portés par **l'organisme international de standardisation (ISO, *International Organisation for Standardization*).**

VII. Les Moyens de protection contre les Attaques

A) Sur le plan organisationnel

1. *Application des grands principes de la sécurité informatique*

a) Amélioration continue de la sécurité (PDCA)

✓ *La roue de Deming*

La roue de Deming est une illustration de la **méthode qualité PDCA** (**Plan Do Check Act**). La méthode comporte quatre étapes, chacune entraînant l'autre, et vise à établir un cercle fermé. Sa mise en place doit permettre d'améliorer sans cesse la qualité d'un produit, d'une œuvre, d'un service...

- **Plan** : ce que l'on va faire.
- **Do** : production.
- **Check** : mesure, vérification.
- **Act** : décision améliorative, corrective.

b) Élaboration d'une Politique de Sécurité du Système d'Information (PSSI)

La politique de sécurité d'un système d'information est un document formel comprenant des directives, recommandations et principes de sécurité applicables à un système d'information pour garantir sa sécurité. Il s'agit d'un document stratégique généralement validé par la hiérarchie de l'organisme ou de l'entreprise.
Ce document vise à démontrer le soutien de la direction en ce qui concerne la gestion de la sécurité.

Une politique de sécurité s'accompagne souvent des exigences de sécurité et des guides de bonnes pratiques visant à mettre en application cette politique de sécurité. De même, une PSSI est appelé à être maintenue. Elle doit évoluer en fonction des changements survenus ou observés dans le Système d'Information.
La révision régulière de la politique de sécurité permet d'assurer sa continuité et son efficacité.

c) Mise en place d'une gestion des risques

En matière de sécurité des systèmes d'information, la gestion des risques est un processus visant à :

- apprécier les risques qui pèsent sur les actifs de l'entreprise, ses valeurs et parfois son personnel,
- traiter les risques appréciés.

Certaines méthodes d'analyse de risques peuvent être utilisées pour élaborer une PSSI.

✓ *La méthode* **MEHARI**

La **MEthode Harmonisée d'Analyse de RIsques** (MEHARI) a été élaborée par la Commission Méthodes du **CLUSIF** (Club de la Sécurité des Systèmes d'Information Français).

Le but de la méthode d'approche top-down est de mettre à disposition des règles, modes de présentation et schémas de décision. L'objectif de la méthode est de proposer, au niveau d'une activité comme à celui d'une entreprise, un plan de sécurité qui se traduit par un ensemble cohérent de mesures permettant de palier au mieux, les failles constatées, et d'atteindre le niveau de sécurité répondant aux exigences des objectifs fixés.

✓ *La méthode MARION*

La méthode **MARION** (**Méthodologie d'Analyse de Risques Informatiques Orientée par Niveaux**) est issue du **CLUSIF**.

Il s'agit d'une méthodologie d'audit, qui, permet d'évaluer le niveau de sécurité d'une entreprise (les risques) au travers de questionnaires pondérés donnant des indicateurs sous la forme de notes dans différents thèmes concourant à la sécurité.

Objectif de la méthode

L'objectif est d'obtenir une vision de l'entreprise auditée à la fois par rapport à un niveau jugé " correct ", et d'autre part par rapport aux entreprises ayant déjà répondu au même questionnaire.

- ✓ ***La Méthode EBIOS*** (**Expression des Besoins et Identification des Objectifs de Sécurité**) est une méthode, préconisée actuellement dans l'administration française, et est constituée de plusieurs guides et repose sur la prise en compte de besoins en sécurité du système d'information.

2. *Application des grands principes de défense*

Les grands principes de défense d'un système d'information peuvent être classés en quatre grandes catégories : Prévention, Protection, Détection et Réaction.

a) *Principe de prévention*

Le principe de prévention consiste à mettre en place des moyens ou dispositifs en vue de prévoir des éventuelles attaques qui pourraient avoir lieu sur le système.

Exemple

Par exemple, le fait de cloisonner un réseau en domaine de sécurité afin d'éviter qu'une attaque sur une partie du réseau n'affecte les autres parties du réseau, fait partie des principes de prévention.

b) Principe de protection

Le principe de protection consiste à mettre en place des moyens ou dispositifs permettant de protéger un bien ou un ensemble de biens (essentiel ou support) du système d'information

Exemple

Par exemple, installer un pare-feu à l'entrée du réseau local d'une entreprise pour assurer le filtrage des paquets entrant et/ou sortant, fait partie des principes de protection contre les attaques.

c) Principe de détection

Le principe de détection consiste à mettre en place des dispositifs matériels et/ou logiciels permettant identifier les intrusions dans un système ou dans une application. Sur le plan logiciel, ce principe s'appuie sur des outils tels que des bases de données, des algorithmes pour détecter les attaques.

Généralement, la procédure de détection est couplée à la procédure d'alerte, ce qui est tout à fait logique, car une détection sans alerte n'apporte pas de valeur ajoutée à la sécurisation d'un système.

Exemple

Par exemple, le fait de mettre en place une caméra vidéo couplée à un déclencheur automatique d'alarme dans un bâtiment en vue de détecter les intrusions physiques, fait partie des principes de détection.

d) Principe de réaction

Le principe de réaction consiste à mettre en place un ensemble de moyens, procédures ou dispositifs (matériels ou logiciels) visant à réagir vis à vis des dysfonctionnements identifiés sur le système. Des procédures de réaction doivent être rédigées de manière non ambiguë, et mises à la disposition non seulement des spécialistes en charge de la sécurité, mais aussi des utilisateurs.

Exemple

Par exemple, réviser les règles de filtrage au niveau d'un **pare-feu** suite à une attaque sur le réseau depuis l'extérieur, fait partie des principes de réaction.

B) Sur le plan technique

1. *Application des mécanismes de sécurité*

Un mécanisme de sécurité peut-être vu au sens large comme une combinaison d'éléments destinés à fonctionner ensemble pour produire un résultat. Dans le cadre d'un système d'information, il s'agit d'un groupe de fonctions ou de moyens ayant un objectif commun.

a) Mécanisme d'authentification

Ce mécanisme permet de vérifier la véracité des utilisateurs, du réseau et des documents. Il est utilisé dans le cadre du contrôle d'accès (physique ou logique).

b) *Mécanisme de chiffrement*

Ce mécanisme permet de rendre inintelligible des informations à ceux qui n'ont pas l'autorisation. Il est utilisé pour assurer la confidentialité des données et la signature numérique.

c) Mécanisme de contrôle d'accès

Ce mécanisme permet d'identifier tous les accès au système. Ces accès peuvent être physiques ou logiques.

d) Mécanisme de filtrage

Ce mécanisme permet de filtrer les paquets ou requêtes provenant d'une source (hôte, réseau), ou alors à destination d'un hôte ou d'un réseau. Il est utilisé par des équipements de filtrage tels que les pare-feu, proxy, etc.

e) Mécanisme de détection

Ce mécanisme permet de détecter des anomalies dans un réseau, un système ou une application. Par exemple la détection des injections de code SQL dans une application.

2. *Application du mécanisme de cloisonnement et du principe de l'architecture n-tiers*

Le cloisonnement fait partie des principes fondamentaux de la sécurité des systèmes d'information. Lorsqu'il est appliqué à un réseau, il consiste à segmenter physiquement ou logiquement le réseau en domaines de sécurité (intranet, Wifi, DMZ, etc..). Les équipements de sécurité tels que les pare-feu, les commutateurs peuvent être utilisés à cet effet.

Lorsqu'il est appliqué à une application, on parle plutôt ***d'architecture applicative ntiers.***

Il s'agit d'une architecture en couches. Ainsi, dans une architecture 3-tiers, on distinguera trois couches :

- ✓ une couche "présentation" qui est chargée de présenter les résultats traités par la couche application. **Exemple : un portail web**
- ✓ une couche "application" qui est chargée de traiter des données et de les mettre à la disposition de la couche présentation.
- ✓ une couche "donnée" qui est chargée de stocker des données brutes ou traitées.

3. *Mise en place des dispositifs de sécurité*

Sur le plan technique, la protection d'un système informatique passe par :

- ✓ La mise en place des dispositifs (matériel ou logiciel) de sécurité tels que les firewalls, IDS(Intrusion Detection System), NIDS(Network Intrusion Detection System), alarme, etc.
- ✓ L'installation et la configuration des logiciels de sécurité tels que les antivirus, anti-spam, etc.
- ✓ Le durcissement (**hardering**) des dispositifs de sécurité, des serveurs et des stations de travail.

- ✓ l'installation et la configuration des dispositifs de contrôle (monitoring) afin de voir ce qui se passe aussi bien sur le réseau que sur les équipements du réseau.

Remarque

Les équipements de sécurité doivent eux-mêmes être protégés et contrôlés afin de s'assurer qu'ils fonctionnent parfaitement. Quant aux logiciels de sécurité, ils doivent être mis à jour régulièrement.

4. Application des correctifs de sécurité

Les logiciels étant développés par des humains, ils sont susceptibles de contenir des erreurs. Lorsque des erreurs (failles) sont découvertes dans un logiciel, des actions sont entreprises par l'éditeur ou le responsable afin de les corriger. Ces corrections sont généralement fournies sous forme de modules appelés "**patches**" ou correctifs.

Il est recommandé de toujours appliquer les correctifs de sécurité aux logiciels, afin d'éviter que les failles ne soient exploitées.

C) Sur le plan de la mise en œuvre opérationnelle

Assurer la sécurité d'un système informatique sur le plan mise en œuvre opérationnelle consiste à prendre en compte tous les aspects en rapport avec la sécurité, avant, pendant et après la mise en production d'un service, d'une application ou d'un équipement.

Ces aspects peuvent porter sur :

- la définition et le suivi des contrats de maintenance avec les fournisseurs,
- l'élaboration des procédures d'acquisition, de mise en place et de maintenance,
- l'élaboration des manuels de procédures et le test de ces procédures. **Par exemple**, les procédures de gestion des incidents de sécurité.
- la sensibilisation et la formation des acteurs du système (responsable, administrateurs, utilisateurs, etc.).
- la réalisation des audits sécurité afin de s'assurer que le niveau de sécurité en place est satisfaisant.
- l'élaboration d'un plan de continuité d'activités etc.