Introduction à la sécurité des échanges

Master Ingénierie des logiciels

10-07-2017
1.0

Table des matières

Introduction à la sécurité des échanges

I

Dans cette partie on présentera les différents défis de la sécurité informatique, les différents types d'attaques et leurs motivations, les services de sécurité, et des statistiques sur les pertes engendrées par des attaques sur les systèmes d'information d'entreprise.

1. Réseaux informatiques : Risques et enjeux

Confiance et Internet

Dans la vie courante la plupart des transactions reposent sur une « confiance » acquise par une relation en face à face ou un contact physique . Dans le cybermonde cette relation de proximité est rompue. Comment établir une relation de confiance indispensable à la réalisation de transactions à distance entre personnes qui ne se connaissent pas ? Ce cours a pour but de répondre à cette question.

Fondamental : Part de responsabilité des usagers

Thucydite dit : « Ce ne sont pas les murs qui protègent la citadelle, mais l'esprit de ses habitants ». Ceci s'applique également aux systèmes d'information où les statistiques indiquent que 40% des attaques sont causées par les usagers du SI eux mêmes.

Rappel : Environnement de l'entreprise

Une vingtaine d'années auparavant, les systèmes d'information d'entreprises étaient plutôt centralisés, basés sur des échange papiers, sans accès distants. Aujourd'hui les SI d'entreprises sont plutôt distribués sur plusieurs sites: on retrouve notamment un siège principales et des succursales, des filiales, des télétravailleurs, des commerciaux, ... L'accès distants devient alors indispensable pour supporter cette décentralisation et la mondialisation des échanges. Ceci devient plus important avec les nouvelles technologies sans fils (Haut débit sur GSM, UMTS, WiMAX, etc.) et la forte pénétration d'Internet dans nos sociétés ;dans quelques années le nombre d'internautes atteindra les 3.000.000.000 de personnes.

Attention : Risques liés aux réseaux

Malgré les bienfaits des réseaux informatiques, ceux-ci présentent d'énormes risques. Parmi ceux-là on peut citer :

- Interception de messages
    - Prise de connaissance des mots de passe
    - Vol d'information
    - Perte d'intégrité du système et du réseau

Malgré la panoplie de technologies utilisées pour sécuriser les SI des entreprises, les attaques sur les SI existent toujours comme illustré dans la figure suivante tirée d'une enquête du FBI/CSI en 2006.

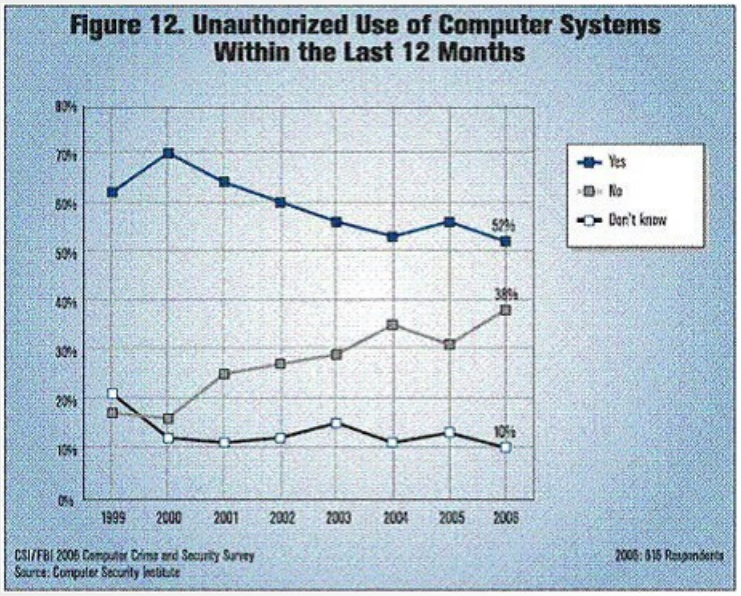

Image 2 : Accès frauduleux aux SI

La figure suivante illustre les différents types d'attaques notées en 2006 :

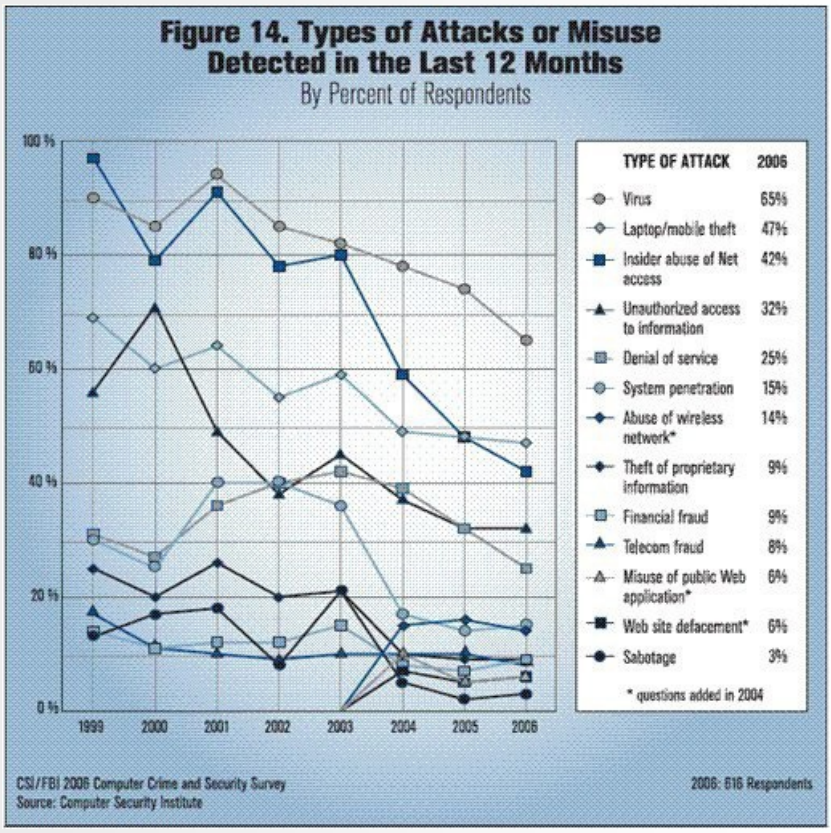

Image 2 : Types d'attaques sur les SI en 2006

Motivations d'un attaquant

Un attaquant n'est pas forcément un "hacker" chevronné. Ca peut être n'importe quelle personne avec des motivations aussi banales que les suivantes :

- Le gain financier
    - Récupération de num de cartes bancaires, ...
- Vengeance
    - Site www.aljazeera.net lors de la couverture de la guerre d'irak
- Besoin de reconnaissance
    - Attaque contre le site du cerist avec un message sur les restrictions d'accès à Internet à Cuba.
- Curiosité
    - Attaques d'étudiants du MIT sur le premier ordinateur IBM 704 au MIT en 1959.
- Recherche d'émotions fortes
- Ignorance
    - Envoie de mots de passes par email, ...

Pertes phénoménales !!!

Les pertes financières dues aux attaques informatiques sont phénoménales. D'après une enquête réalisée par le FBI/CSI :

- attaques de virus (plus de 15 millions de dollars de perte)
- accès non autorisés aux systèmes d'information (plus de 10 millions de dollars de perte)
- vols d'équipement mobile (plus de 6 millions de dollars)
- vols de la propriété intellectuelle (plus de 6 millions de dollars)

52% des organisations sondées ont déclaré avoir été attaqué les 12 derniers mois (2006) :

- 24% d'entre elles ont reporté plus de 6 attaques
- 48% ont reporté 1 à 5 attaques

La figure suivante illustre la répartition des pertes sur leurs causes :

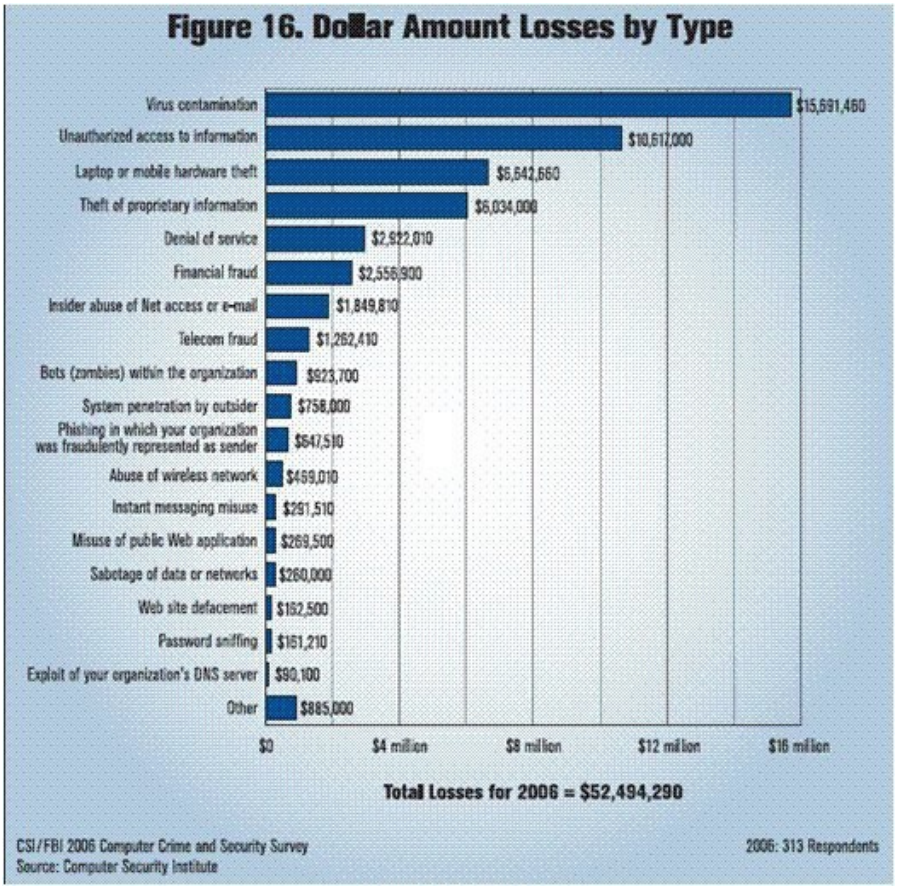

Image 3 : Pertes financières

Complément : Rehaussement des budgets réservés à la sécurité des SI

La conséquence immédiate de ces pertes qui sont majoritairement liées à la sécurité des SI, est l'augmentation importante des budgets alloués à sécuriser les SI et à former le personnel sur la sécurisation des SI et des échanges d'information. Selon la même enquête :

- 34% des organisations allouent pas moins de 5% du budget informatique à la sécurité informatique
    - En 2006, les compagnies de revenues inférieurs à 10 millions de dollars ont dépensé en moyenne 1349 dollars par employé pour la sécurité informatique- un rehaussement de 210% par rapport à l'année 2005
- plus de 80% des institutions conduisent un audit de sécurité informatique
- la majorité des institutions jugent la formation en sécurité informatique comme importante et stratégique
    - 61% de ces organisations refusent de sous-traiter leurs fonctions de sécurité informatique

La figure suivante illustre le pourcentage du budget IT alloué à la sécurité :

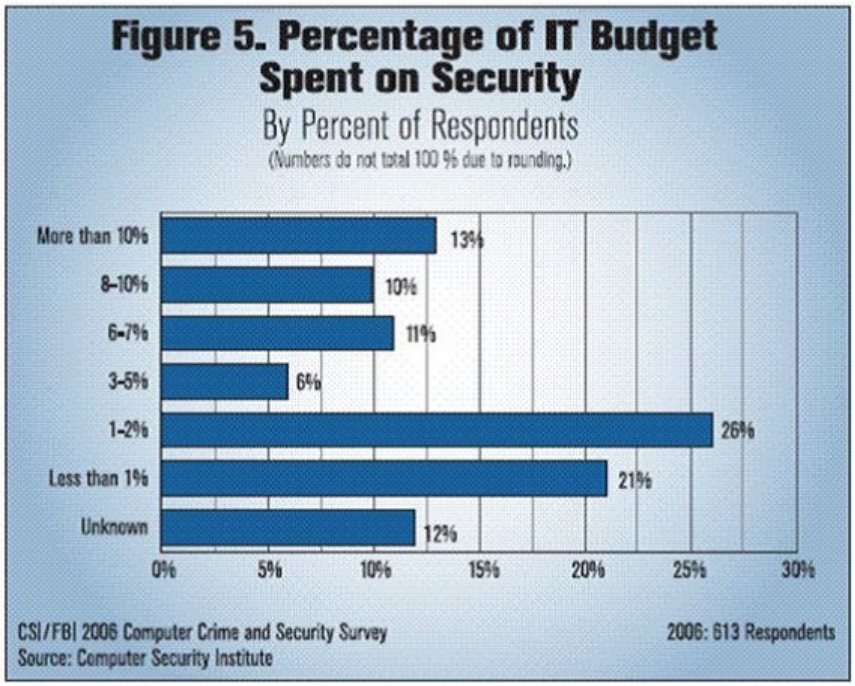

Image 4 : Part de la sécurité dans le budget IT

Remarque : Rapport du FBI/CSI

Le FBI/CSI (Computer Security Institute) publie chaque année un rapport sur la sécurité informatique. Voici le rapport du FBI/CSI pour 2007 :

Exemple : Menaces Informatiques et Pratiques de Sécurité en France

Selon un le rapport 2008 du CLUSIF (Club de la Sécurité de l'Information Français) :

- Plus de 70% des entreprises françaises ont une forte dépendance à l'informatique
- Le budget moyen alloué pour la sécurité du SI dépasse 114K€ dans 21% des cas.
- 28% des entreprises du secteur des services, banques et assurances ont augmenté leur budget sécurité du SI de plus de 10% en 2008
- 53% des Responsables de Sécurité du SI (RSSI) dénoncent le manque de personnel qualifié comme frein majeur à la conduite de leur mission.
- Plus de 30% des entreprises n'ont pas une Politique de Sécurité de l'Information (PSI), et 45% de celles qui en ont ne respectent pas une norme de sécurité.
- Le rattachement de la RSSI à la DG passe de 39% en 2006 à 45% des cas en 2008.

Selon le même rapport du CLUSIF, beaucoup de technologies de contrôle d'accès sont méconnues et/ou non utilisées en entreprises françaises comme illustré dans la figure suivante :

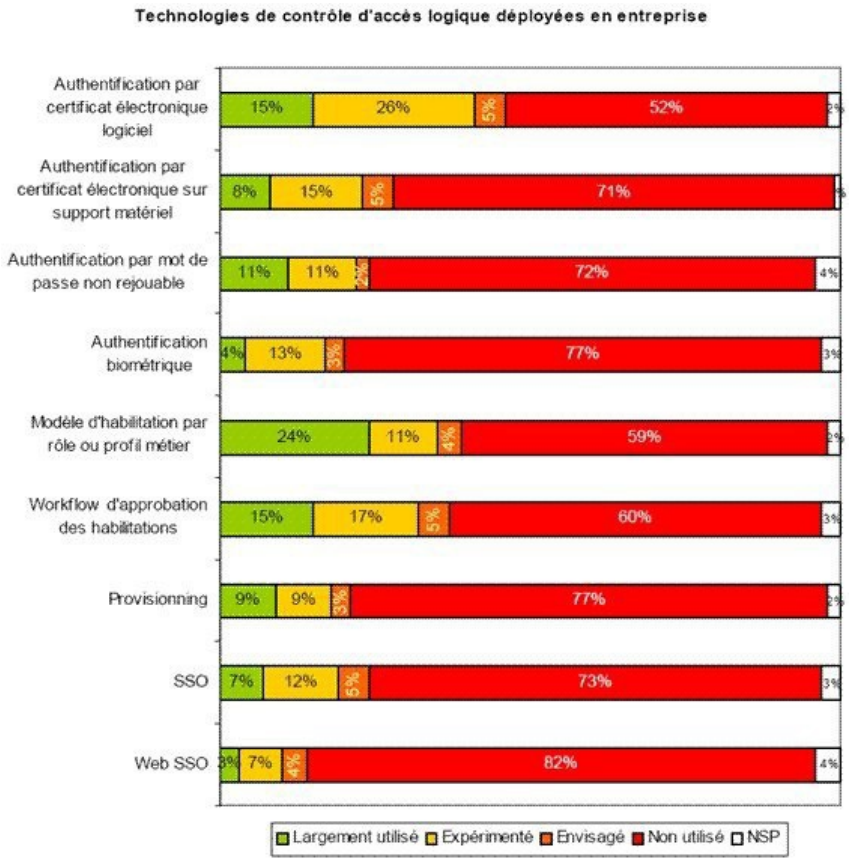

Image 5 : Technologies de contrôle d'accès non utilisées en France

Le rapport note aussi que 56% des RSSI ont noté au moins un incident de sécurité

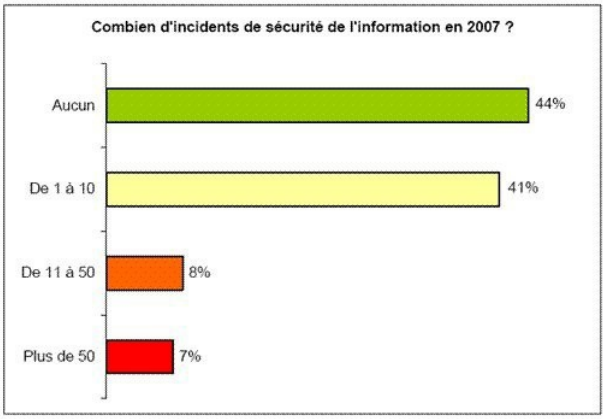

Image 6 : Incidents de sécurité informatique en France

Le rapport du CLUSIF 2008 est très riche et mérite une lecture. Le voici :

2. Définitions des Services de Sécurité

Voici quelques définitions informelles à retenir concernant les services de sécurité

les plus importants

Définition : Authentification

Permet de vérifier l'identité revendiquée par une entité, ou l'origine d'un message, ou d'une donnée .

Définition : Confidentialité

Permet de se protéger contre la consultation abusive des données par des entités tierces indésirables

Définition : Contrôle d'intégrité

Permet de vérifier qu'une données n'a pas été modifiée par une entité tierce (accidentellement ou intentionnellement)

Définition : Contrôle d'accès

Permet de vérifier que toute entité n'accède qu'aux services et informations pour lesquelles elle est autorisée

Définition : Non répudiation

Permet de se protéger contre la contestation d'envoi et de réception de données lors d'une communication