Sécurité informatique: introduction

License Pro

Renaud Tabary: tabary@enseirb.fr

2008-2009

Plan

Définition de la sécurité informatique

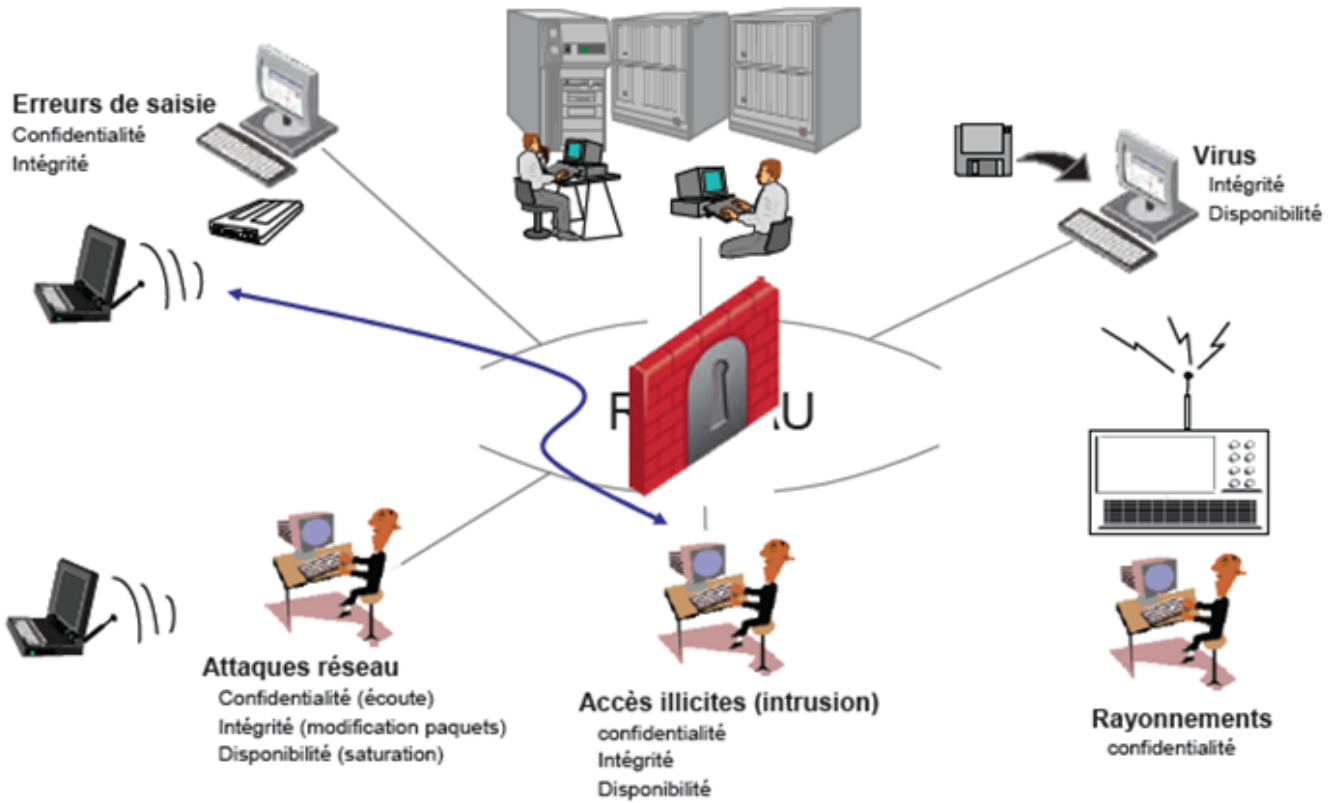
Definition

Information security is the protection of information [Assets] from a wide range of threats in order to ensure business continuity, minimize business risks and maximize return on investment and business opportunities.

Sécurité informatique

- Les systèmes informatiques sont au coeur des systèmes d'information
- Ils sont devenus la cible de ceux qui convoitent l'information
- Assurer la sécurité de l'information implique d'assurer la sécurité des systèmes informatiques

La sécurité des systèmes d'informations



Qui sont les pirates ?

- Peut être n'importe qui avec l'évolution et la vulgarisation des connaissances
- Beaucoup d'outils sont disponibles sur Internet
- Trois générations :
  - 80's-90's : techniciens éclairés
  - 1990-2000 : script kiddies
  - 2000-aujourd'hui : l'insécurité devient facilement rentable
    - Pub, SPAM
    - e-commerce
    - Espionnage industriel

Quels sont leurs objectifs

Objectifs des attaques :

- Prouver ses compétences techniques
- Représailles
- Désinformer (ex : Amazon)
- Empêcher l'accès à une ressource (Bombes logiques, DOS)
- Prendre le contrôle d'une ressource (BotNets)
- Récupérer de l'information sur un système (Espionnage industriel)
- Générer des revenus : (Vol, Extorsion, Publicité)

Les risques pour l'entreprise

Les risques encourus par l'entreprise :

- Les risque stratégiques
  - Destruction/altération de données
    - Exemple : `Boeing` (57000$ après une intrusion)
  - Vol de données stratégiques
    - Exemple : `Gartner William Malik` (900 M$)
- Les autres risques
  - Le commerce electronique
    - Exemple : `Kevin Mitnick` et `Netcom`
  - Piratage de site web
    - Image de marque, militantisme

La sécurité, un marché porteur

Selon IDC 2005[101]

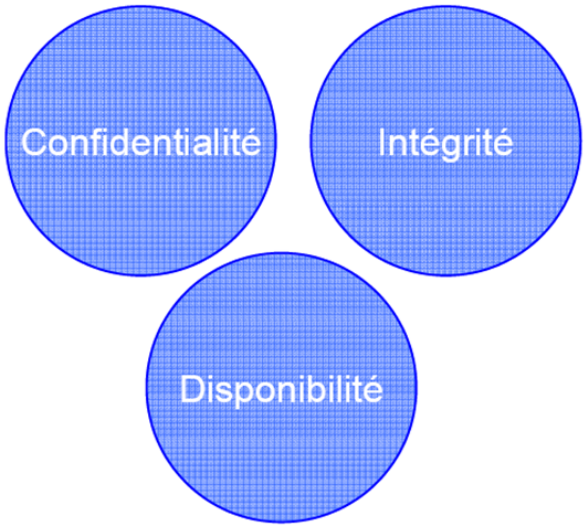
Segment	Croissance du marché/an (2004-2009)	Marché national (M€) en 2004	Principaux acteurs	Présence française	Produit logiciel libre public	Criticité des produits
Logiciels : Anti–virus, Anti-spam et Spyware (segment SCM[102])	16%	157	Symantec, Network Associates (MC Afee), Trend, Sophos ...	Non	Oui, ClamAV	Non
Pares – feu / VPN (appliances)	2%	47	Check Point, Cisco,...	PME	Oui, netfilter, IP filter	Oui
Pares-feu (logiciels)	5%	44				Oui
Prévention et détection d'intrusion (appliances)	22%	11	Symantec et Internet Security Services (50% du marché à 2)	PME	Oui, Snort	Oui
Administration sûre (3A)[103]	13%	88	IBM, Computer Associates, Verisign,...	GE[104] et PME		Oui

Plan

Objectifs

Les trois princpaux objectifs de la sécurité infromatique :

- **Confidentialité**
- **Intégrité**
- **Disponibilité**



Confidentialité

Definition

Propriété d'une donnée dont la diffusion doit être limitée aux seules personnes autorisées

Menaces :

- Ecoute du réseau
  - Interne
  - Externe
- Vol de fichiers
  - Données
  - Mots de passe
- Espionnage
- Ingénierie sociale

Contre-mesures :

- Cryptographie (chiffrement)
  - Des données
  - Des communications
- Contrôle d'accès
  - Logique (mot de passe)
  - Physique (biométrie)
- Classification des actifs
- Formation du personnel

Intégrité

Definition

Propriété d'une donnée dont la valeur est conforme à celle définie par son propriétaire

Menaces :

- Attaques malicieuses
  - Vers, virus
  - Bombes logiques
- Désinformation
- Erreurs humaines

Contre-mesures :

- Cryptographie
  - Signature, authentification
- Systèmes de détection
  - Antivirus, systèmes de détection d'intrusion (IDS)
- Politique de sauvegarde

Disponibilité

Definition

Propriété d'un S.I capable d'assurer ses fonctions sans interruption, délai ou dégradation, au moment même où la sollicitation en est faite

Menaces :

- Attaques malicieuses
  - Denis de services
  - SPAM
- Attaques accidentelles
  - Le *"Slashdot effect"*
- Pannes

Contre-mesures :

- Pare-feu
- Systèmes de détection d'intrusions
- Clustering
- Formation des administrateurs

Les actifs de l'entreprise

Que protéger ?

Definition

Les actifs informationnels représentent l'ensemble des données et des systèmes de l'information nécessaires au bon déroulement d'une entreprise

- Base de données clients
  - Vente et Marketing
- Base de données des employés
  - Ressources humaines
- Portail web
  - Vente
- Codes sources
  - Equipe de developpement
- Base de données usagers
  - Equipe système

Objectifs (reformulés) :

- La sécurité de l'information consiste à protéger les *actifs* informationnels afin d'assurer l'intégralité de leurs *propriétés*
- Les actifs et leurs propriétés sont définis par les *objectifs d'affaire*

Plan

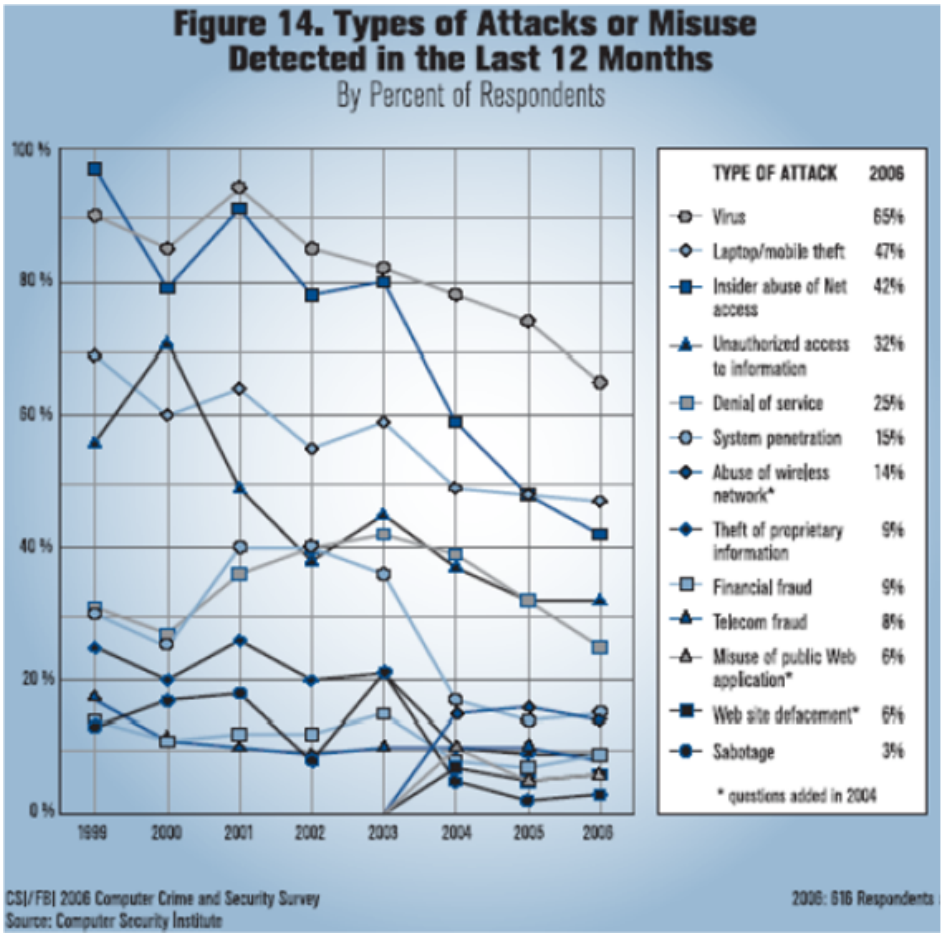
Un constat amer

Evolution des risques :

- En 2005, sur 218 entreprises européennes, plus de 50% ont subit des pertes financières liées à des attaques informatiques
  - Croissance de l'Internet
  - Ouverture des réseaux de communication
  - Succès des technologies nomades (téléphones, pda)
  - Augmentation du nombre d'attaques
  - Technologies plus complexes et moins maitrisées
  - Changement de profil des pirates

Type des attaques

Types d'attaques répertoriées en 2006 :

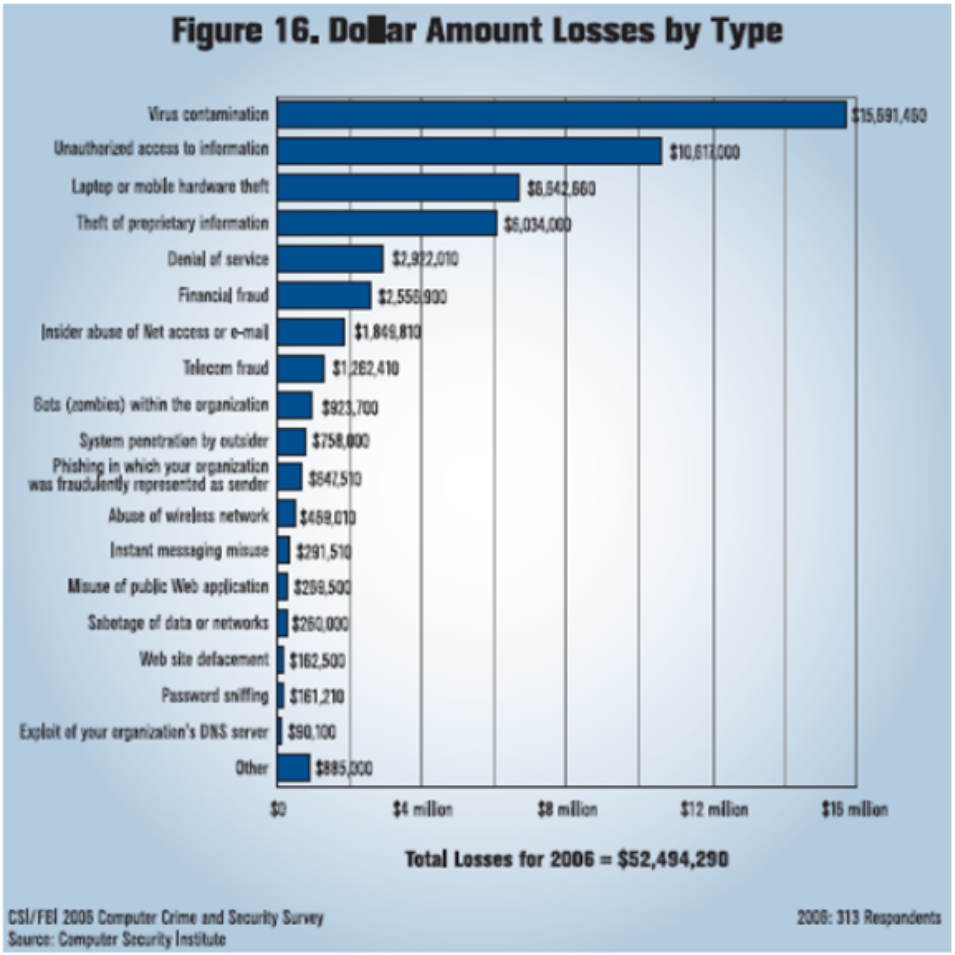


Délais des attaques

Evolution des délais entre découverte d'une vulnérabilité et exploitation :

Nom	Annonce	Exploit	Intervalle
SQLsnake	27 novembre 2001	22 mai 2002	176
CodeRed	19 juin 2001	19 juillet 2001	30
Nimda *Plusieurs vecteurs*	▪15 mai 2001 ▪6 août 2001 ▪3 avril 2001	18 septembre 2001	▪126 ▪42 ▪168
Slapper	30 juillet 2002	14 septembre 2002	45
Scalper	17 juin 2002	28 juin 2002	11

Les coûts de l'insécurité



Plan

Définition

Definition

Les politiques de sécurité sont des énoncés généraux dictées par les cadres supérieurs décrivant le rôle de la sécurité au sein de l'entreprise afin d'assurer les objectifs d'affaire.

- Pour mettre en oeuvre ces politiques, une organisation doit être mise en place.
- Définition des rôles, des responsabilités et des imputabilités

Politique de sécurité

Compromis sécurité - fonctionnalité :

- Définir les besoins.
  - Déterminer les actifs à protéger et leurs propriétaires
    - Quelles sont leurs valeurs ? Quelles sont leurs criticités ? Quelles sont leurs propriétés ?
  - Déterminer les menaces représentant des risques
    - Quels sont les acteurs ? attaqueurs ? Quels sont leurs moyens ?
  - Déterminer les objectifs à atteindre
    - Quelles sont les propriétés des actifs à protéger ?
- Proposer une solution.
  - Déterminer les contre-mesures à mettre en place
- Évaluer les risques résiduels.
  - Déterminer quelles sont les vulnérabilités toujours présentes
  - Déterminer leurs impacts sur les objectifs initiaux

Politique de sécurité (2)

Création d'une politique de sécurité :

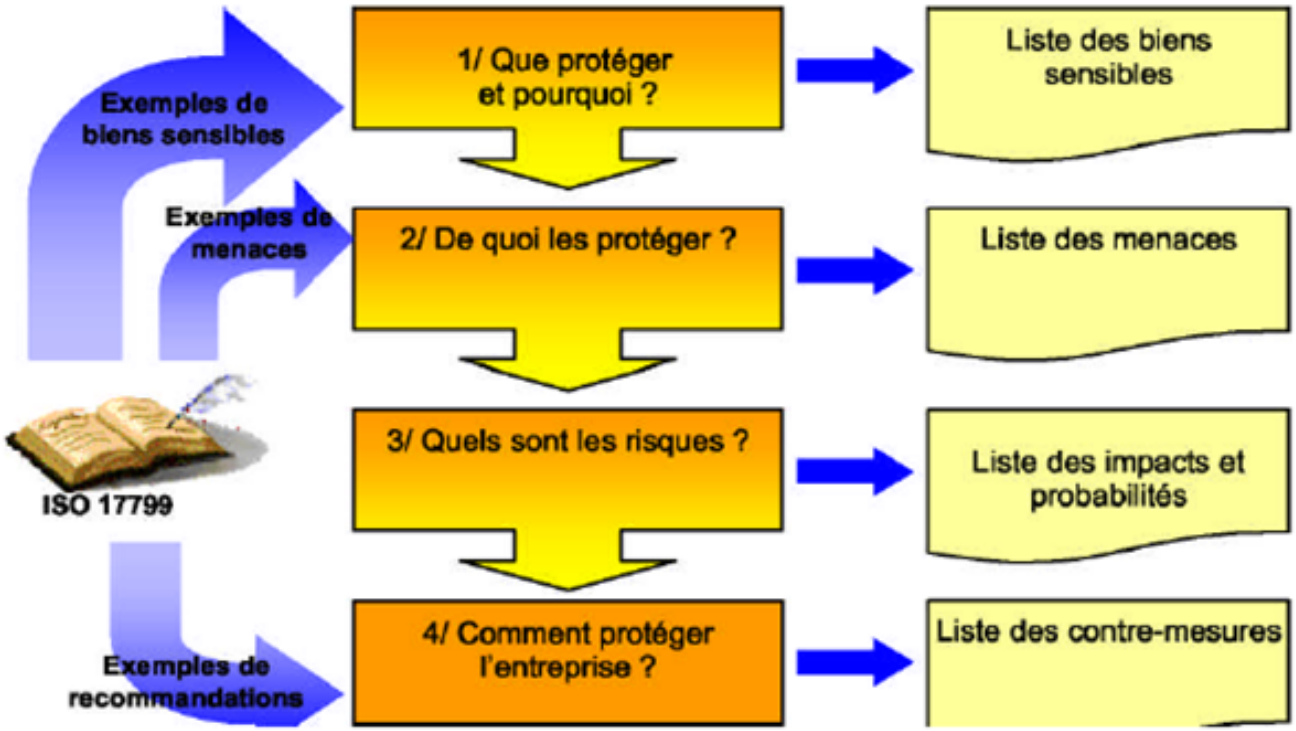
- Mise en oeuvre
- Audit
- Tests d'intrusion
- Détection d'incidents
- Réactions
- Restauration

Politique de sécurité (3)

Quelques méthodes :

- EBIOS (Expressions des Besoins et Identification des Objectifs de Sécurité) http ://www.ssi.gouv.fr/fr/confiance/ebios.html
- MEHARI (MEthode Harmonisée d'Analyse de Risques) http ://www.clusif.asso.fr/fr/production/mehari
- Critères Communs (http ://www.commoncriteriaportal.org)
- La norme ISO 17799 Présentation : http ://www.clusif.asso.fr/fr/production/ouvrages/pdf/Presentation-ISO17799-2005.pdf

Exemple ISO 17799



Plan

Logiciel de sécurité par excellence ?

- Pare-feu ?
- Antivirus ?
- Système de détection d'intrusions ?
- . . . ?
- **PowerPoint** ! ! !

Le problème

L'industrie de la sécurité

- En 2003, le marché de la sécurité réseau était évalué à 45 milliards USD
- Constat
  - L'approche traditionnelle de sécuriser le périmètre du réseau ne semble pas adéquate puisque nous avons toujours les mêmes problèmes
- Raisons :
  - Le manque d'information des utilisateurs
  - La **qualité des logiciels**

Le rôle du développeur

- La sécurité des logiciels est donc critique !
  - 50 % des vulnérabilités proviennent des erreurs de conception
  - 50 % des vulnérabilités proviennent des erreurs d'implémentation
    - Dépassement de mémoire et d'entier
    - Concurrence critique
- Microsoft's Trustworthy Computing Initiative
  - Mémo de Bill Gates en janvier 2002 présente la nouvelle approche de Microsoft de développer des logiciels sécurisés
  - Microsoft aurait dépensé plus de 300 millions USD
- Workshop on Rapide Malware 2006
  - Un panel reconnaissait l'impact de cette initiative sur la prévalence des vers et des virus

Solution

Plusieurs solutions :

- Développement fiable (cycle en V, en W, etc.)
- Politique qualité au sein de l'entreprise (ISO, CMMI)
- **Informer** !

Plan

Conclusion

- La sécurité informatique ne doit plus être ignorée !
- Connaissez-vous vous-même
  - Déterminer les actifs qui doivent être protégés et leurs propriétés
  - Déterminer les objectifs à atteindre
- Connaissez vos ennemis
  - Déterminer les menaces contre lesquelles ils doivent être protégés
- Réagissez !
  - Politique de sécurité
  - Principes, guides et règles connues
  - Informer

Plan

Liens utiles

- http ://www.miscmag.com (FR)
- http ://sid.rstack.org/blog (FR)
- http ://www.securityfocus.com
- http ://www.sans.org
- http ://www.hoobie.net
- http ://packetstorm.security.org
- http ://www.rootshell.com
- et beaucoup d'autres ...