Technologies et Marché de l'informatique :

CSI/FBI

"Computer Crime and Security Survey"

Jerôme Herbault	herbau_j
David Lorin	lorin_d
Pierre-Yves Rofes-Vernis	rofes-_p
Stéphane Roissard	roissa_s

Introduction

- Sondage organisé par le Computer Security Institute en association avec le Bureau Fédéral d'Investigation de San Francisco .
- 11ème parution en 2006
- Le questionnaire porte principalement sur les incidents , attaques et crimes informatiques qu'ont subit les entreprises concernées.

Profil des participants 1/2

- Grande variété dans les secteurs représentés
- Proportions égales de petits et de grand comptes
- Néanmoins la proportion effectives de ces entreprises étant très différente les grands comptes interviennent dans cette étude de manière plus significative

Profil des participants 2/2

- Jusqu'en 2005 : diminution très nette des déclarations aux autorités des incidents de sécurité.
- Depuis 2006 : reprise significative des déclarations.
- Résistance toujours très forte des entreprises de rendre public les incidents dont elle a été victime à cause de l'image négative que cela engendre.

Dépenses liées a la sécurité

- Evolution de la part consacrée du budget info en sécurité:

Année	Moins de 2%	8% ou plus
2004	40	16
2005	35	19
2006	47	23

- Sensibilisation d'une bonne partie des societes, mais pas toutes.

Évolution des Technologies

- Usage répandu et stable des technos « classiques »: FireWall (99%), Antivirus (99%), IDS (70%), IPS (40%)
- Augmentation de la biometrie
- 2006 marque l'arrivee de nouvelles technos: Outils d'analyses Forensics, analyse de logs, equipements dedies pour le Wifi, Firewalls de niveau applicatif

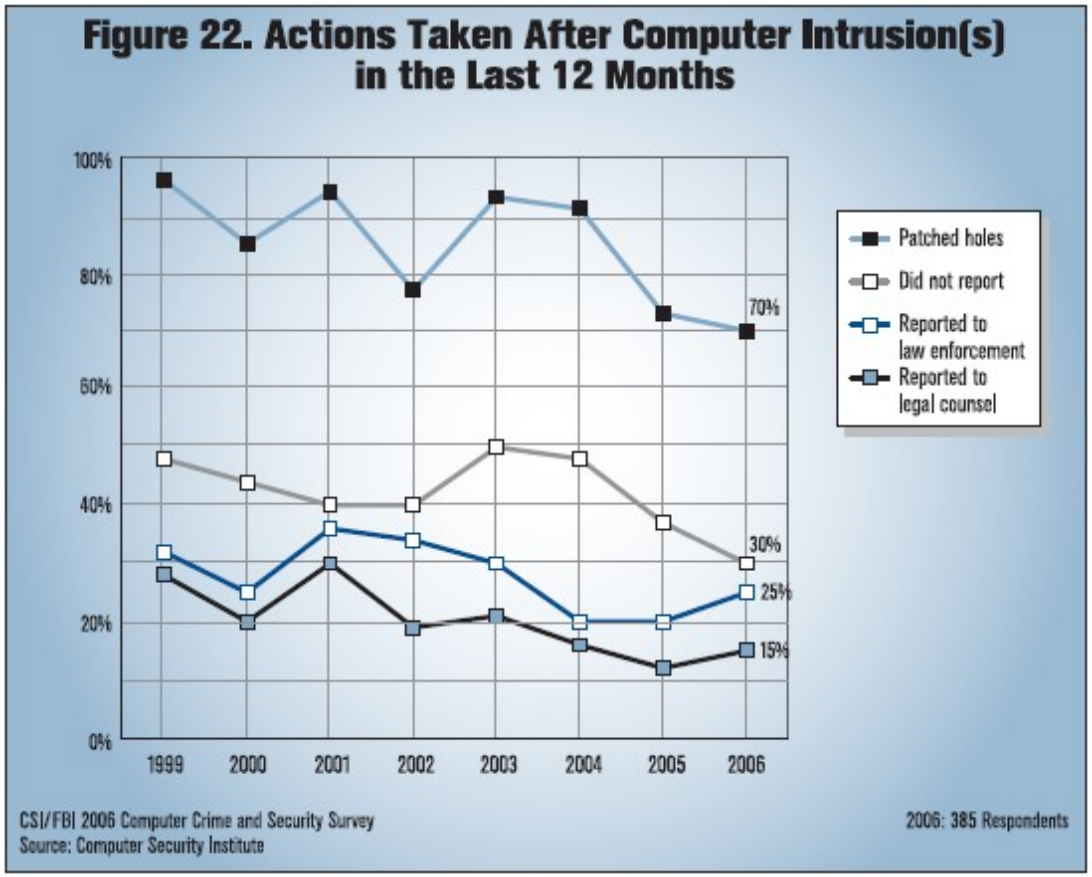
L'Evolution des types d'attaques

- Palmarès 2004 :
  - 78% Virus
  - 59% Abus interne de l'accès Internet
  - 49% Vols des téléphones et ordinateurs portables
- Palmarès 2005 :
  - 75% Virus
  - 50% Vols des téléphones et ordinateurs portables
  - 50% Abus interne de l'accès Internet
- Palmarès 2006 :
  - 65% Virus
  - 47% Vols des téléphones et ordinateurs portables
  - 42% Abus interne de l'accès Internet

Les attaques les plus coûteuses

- 2004 :
  - Denial Of Service $26M
  - Vol de données $11M
  - Abus interne de la connection Internet $10M
  - Abus du réseau Wireless $10M
- 2005 :
  - Virus $42M
  - Accès non authorisé $31M
  - Vol de données $30M
  - DOS 7$
  - Abus interne de la connection Internet 6$
- 2006 :
  - Virus $15M
  - Accès non autorisé à des informations $10M
  - Vol de téléphones ou ordinateurs portables $6M
  - DOS $3M

Comportement après une attaque



Comportement après une attaque

- Pourquoi ne pas rapporter systématiquement une attaque?
  - 48% pour ne pas se faire une mauvaise publiclité
  - 36% ne pas être utilisé à leur avantage pas les concurents

La loi Sarbanes-Oxley

Objectif, principe, et impact sur la sécurité des systèmes d'information

Présentation

- Adoptée en juillet 2002 par le Congrès américain
- Obligation pour les entreprises de procéder à l'analyse de leurs procédures financières et de publier les résultats dans les plus brefs délais
- Réponse à un certain nombre de scandales (Enron, Tyco International, WorldCom, …)

Objectif

- Restaurer la confiance des investisseurs
- Renforcer la gouvernance d'entreprise

Principe

- Garantie d'une présentation adéquate des rapports financiers
- Mise à disposition de processus d'alerte
- Obligation de certifier les rapports financiers par le PDF et le CFO
- Renforcement des contrôles liés au processus de reporting financier

Impact

- Au départ, surtout le secteur financier
- Par la suite, de plus en plus de secteurs prennent conscience de l'impact de la loi

- Evaluation des problèmes de sécurité les plus critiques dans les années à venir :
  1. Protection des données
  2. Conformité aux différentes lois et politiques

Conclusion

- Evolution des mœurs
- Augmentation des dépenses
- Les attaques en vogue

Questions ?

EPITA