

Secured Data Management

Gestion sécurisée du stockage de l'information

Partie 1

Rappels sur les principes de sécurité

One old truism in security is that the cost of protecting yourself against a threat should be less than the cost of recovering if the threat were to strike you.

Politique de sécurité

Enjeux

Objectifs de la présentation

- Rappeler les enjeux de la sécurité
- Chiffrer le coût de la sécurité et le coût des incidents de sécurité
- Donner un aperçu des menaces potentielles
- Bannir quelques fausses idées

Chiffres clefs : incidents en 2005 dans les mairies de plus de 30000 h

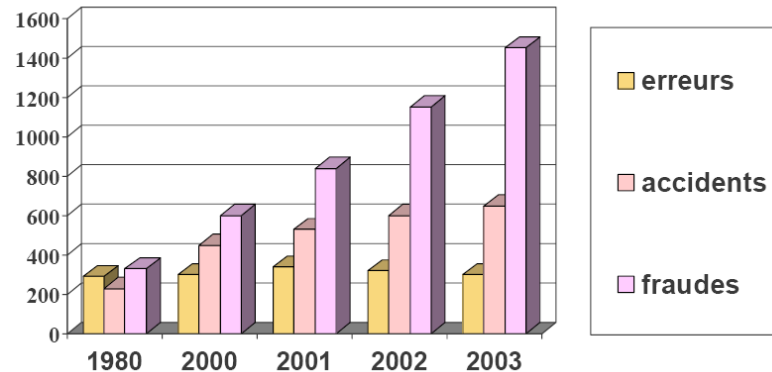
- 60% : vols ou disparition de matériel
- 58% : pannes d'origine interne
- 50% : erreurs humaines d'utilisation
- 48% : pertes de services essentiels dues à des coupures
- 48% : erreurs dans la mise en oeuvre des logiciels ou procédures
- 26% : infection virale
- 18% : événements naturels
- 8% : accidents physiques
- 2% : intrusions dans le SI via dispositif sans fil
- 2% : divulgations d'informations
- 2% : attaques logiques (Ddos...) ciblées
- 2% : actes de dénigrement en ligne (défiguration de sites)
- 0% : sabotages physiques
- 0% : fraudes informatiques ou télécoms
- 0% : actes de chantage

Chiffres clefs : incidents en 2005 dans les entreprises

- 60% : erreurs dans la mise en oeuvre des logiciels ou procédures
- 47% : pertes de services essentiels dues à des coupures
- 46% : erreurs humaines d'utilisation
- 37% : pannes d'origine interne
- 36% : infection virale
- 8% : événements naturels
- 6% : accidents physiques
- 4% : divulgations d'informations
- 4% : attaques logiques (Ddos...) ciblées
- 3% : actes de dénigrement en ligne (défiguration de sites)
- 3% : sabotages physiques
- 2% : intrusions dans le SI
- 2% : fraudes informatiques ou télécoms
- 1% : actes de chantage

Coûts des incidents en France

- En million d'euros pour la France



- Coût moyen d'un incident de sécurité : **70 000 €**
- Dans 20% des cas, plus d'une semaine pour revenir à une situation normale

Menaces informatiques

- Les robots
- Les virus
- Les troyens
- Les bombes logiques
- Les espionlogiciels
- Les canulars (hoaxes)
- Les Keyloggers
- Les vers (worms)
- Le spamming
- Les espions publicitaires
- Rootkits

Robots

- Programmes malveillants permettant une prise de contrôle à distance
- Création de botnet, réseau d'attaque caché
- Implantation par :
 - Spam
 - Vers, virus
 - Cheval de troie
 - Autre robot
- Propagation via :
 - Vulnérabilité
 - Partages ouverts
 - Mots de passes faibles ou manquants

Robots

- 25 à 50 nouveaux robots par jour !
- Contrôle du Botnet depuis serveurs Irc
- Objectifs :
 - Capture d'information
 - Attaques groupées (Ddos)
 - Relais spamming/phishing
 - Diffusion de adwares

Robots : menace réelle

- En 2005, arrestation de plusieurs pirates utilisant ou louant des botnet de plusieurs dizaines de milliers d'ordinateurs
- En octobre 2005, arrestation de 3 hollandais ayant sous leur contrôle quelques ... 1,5 millions de machines et serveurs !!

Robots : exemple à la réunion

- Attaque Ddos sur E-Bay et Yahoo en 2002
- Quelques entreprises à la réunion participe malgré elles à l'attaque
- Poursuites engagées par Yahoo, blacklistage des mails, fermeture des accès, enquête des RG ...

Chevaux de Troie

- Backdoor : programme implémenté secrètement sur une machine et permettant à son concepteur de s'y introduire à distance
- Keylogger : saisie de frappes au clavier et collecte d'informations sensibles. Les données sont ensuite envoyées et employées à des fins frauduleuses.

Chevaux de Troie : exemples

- En Israël : attaques ciblées par chevaux de troie spécifiques (via CD ou Spam). Une fois installé, les accès sont revendus 3000 € à des clients.
- En GB : tentative de détournements de fonds (400 Millions €) dans une banque. Utilisation d'un Keylogger matériel.

Rootkits

- Programme permettant de rendre totalement furtif un autre programme en les rendant invisibles aux outils de sécurité.
- Rend invisibles les processus, les fichiers et les connexions réseaux.
- Difficile à détecter par les anti virus
- Existe historiquement dans le monde libre, mais de plus en plus dans le monde Windows (FURootkit, IsPro, Sony BMG ...)

Idées fausses

- La sécurité coûte chère
- Les intrusions de l'externe sont la principale menace
- La technologie résout la majorité des problèmes de sécurité
- Les approches par les bonnes pratiques sont peu efficaces
- Les logiciels libres sont plus sécurisés
- Un utilisateur ne peut pas être infecté en surfant sur le Web
- La sécurité est la responsabilité du DSI
- La sécurité ne me préoccupe pas, je suis trop petit et je n'ai pas d'informations intéressante à voler
- Un firewall, un antivirus et un IDS garantissent ma sécurité.
- ...

Informations complémentaires

- www.cert.org/archive/pdf/ecrimesummary05.pdf
- www.gocsi.com
- www.clusif.com
- www.mag-securs.com
- solutions.journaldunet.com