Sécurité de l'Information & Contre-Intelligence

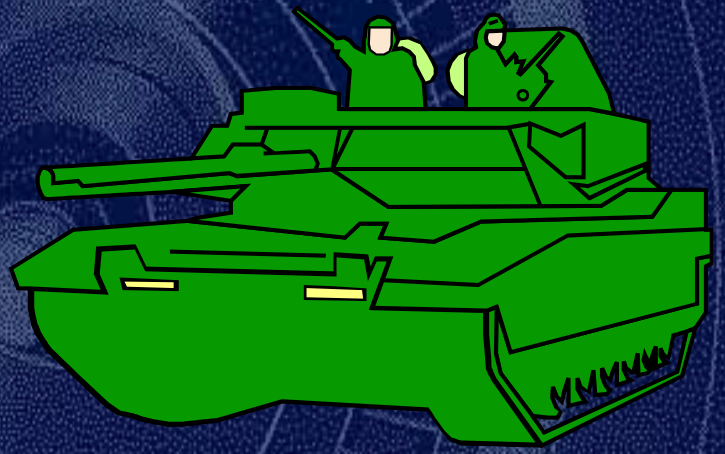
SOLUTIONS BUSINESS

Marc BORRY

1. Introduction

- Sécurité :
  - 1. Situation dans laquelle qqun qqch n'est exposé à aucun danger, à aucun risque d'agression physique, d'accident, de vol, de détérioration
  - 2. Situation de qqun qui se sent à l'abri du danger, qui est rassuré

Une utopie ?



Les enjeux

- Cela n'arrive qu'aux autres
- Discrétion des auteurs et des vicitimes (chiffre noir)

2. Les composantes de la sécurité

- 2.1. Technologique
- 2.2. Technique
- 2.3. Informationnelle

2.1. La composante technologique

- la cybercriminalité

"Le crime informatique est tout acte intentionnel associé d'une manière ou d'une autre aux ordinateurs, dont la victime a ou aurait pu subir une perte, et dont l'auteur a ou aurait pu subir un gain"

Donn Parker

Les attaques

- Pénétration du réseau (hacking)
- Blocage du serveur (bombardement par des paquets d'informations)
- Atteinte aux données (virus, spyware, trojan,…)

Les parades

- Firewall
- Anti-spam
- Logiciels anti-virus (actualisation)
- Modifications des mots de passe
- Cryptage

2.2. La composante technique

- Toutes les précautions du monde ne peuvent vous protéger des erreurs en amont.

Les attaques

- La fraude
- La falsification

Les parades

- L'identification
- L'authentification

2.3. La composante informationnelle

- Vulnérabilité de l'être humain (le capital intellectuel)
- Limite des technologies (exemple des banques)
- Besoin de communication (monde commercial, scientifique,…)
- Modification des habitudes (le FBI et son bibliothécaire électronique)

Les attaques

- Les voyages et les hôtels
- Les foires et expositions
- Les communications et les bavardages
- La gestion des licenciements et des départs
- Les étudiants et les journalistes
- Les faux cabinets d'embaûche
- Les rumeurs, hoax, désinformations

Les parades

- L'audit de sécurité
- Le plan de sécurité global et systématique
  - 27 % des entreprises françaises ont une politique de sécurité globale
  - 20 % réalisent un audit de sécurité
- La stratégie de contre-intelligence

3. L'arme de l'information

- De la stratégie à l'espionnage

- Affaire Perrier
- Commission Rogatoire Internationale
- Rétention de PC à la douane
- Affaire SNECMA / Messier-Dowty
- Opérations Azalée, Caribou et Café noir
- Echelon

4. L ’audit de sécurité

- Identifier les menaces et les agresseurs potentiels
  - Stratégie de l’entreprise ?
  - Inventaire du patrimoine
  - Identification des risques et failles
  - Imaginer les motivations de l’agresseur
  - Risques de complicité interne
  - Retours d’expérience

  … pour établir un plan global de sécurité

5. La stratégie de contre-intelligence

- Etablir les éléments à protéger, les étapes de la démarche et les règles à suivre
- Méthodologie en 10 points

La stratégie de contre-intelligence

1. Tenir à jour une liste des vulnérabilités et risques potentiels

   - stockage des données
   - personnes sensibles
   - étapes critiques

La stratégie de contre-intelligence

2. Protéger les systèmes informatiques de l'intrusion et de l'infection

- protéger les bases de données
- gérer la sauvegarde
- solution anti-virus
- cryptage

La stratégie de contre-intelligence

3. Assurer la confidentialité des données et des documents

- classifier, gérer et protéger
- niveaux de confidentialité
- documents sensibles
- protection des locaux
- documents abandonnés

La stratégie de contre-intelligence

4. Sensibiliser et former le personnel

- sensibilisation
- formation
- responsabilisation
- politiques de sécurité

La stratégie de contre-intelligence

5. Gérer la communication externe

- vérifier les acteurs externes
- clauses de confidentialité
- liste des interventions
- qualification des personnes

La stratégie de contre-intelligence

6. Gérer les visites dans l'entreprise

- identifier
- différencier interne/externe
- liste préalable
- réponses aux questions

La stratégie de contre-intelligence

7. Mettre en place des procédures de sécurité

- endroits appropriés
- contrôle des accès
- choix du mode de communication
- origine douteuse
- code éthique
- charte "sécurité"

La stratégie de contre-intelligence

8. Personnifier la fonction sécurité

- désignation des responsables
- coordination
- audits de sécurité réguliers

La stratégie de contre-intelligence

9. Anticiper les crises

- cellule de crise
- qui fait quoi dans quelles conditions et avec quels délais ?

La stratégie de contre-intelligence

10. Développer une politique de contre-information

- arguments face aux attaques

Sites Internet

- Institut de la Cybercriminalité : www.cybercriminstitut.com
- Protection des données personnelles et voir comment on est pisté sur Internet : www.cnil.fr
- Sécurité des systèmes d'information : www.clusif.asso.fr
- La chasse aux rumeurs et à la désinformation www.hoaxbuster.com
- Sécurité de l'information : www.cnrs.fr/infosecu

Bibliographie

- Longeon Robert, Archimbaud, Jean-Luc, Guide de la sécurité des systèmes d'information à l'usage des directeurs, CNRS , 1999
- Auer François, Comment se protéger de l'espionnage, de la malveillance et de l'intelligence économique, Secret Consulting, 1997
- Etude et Statistiques sur la sinistrabilité informatique en France – 2000, CLUSIF / GMV Conseil, 31 mai 2001

Bibliographie

- Rosé Philippe, la criminalité informatique à l 'horizon 2005 : analyse prospective, Ed. IHESI & L 'Harmattan, 1992

- Marti Yves-Michel, Martinet Bruno, L'Intelligence Economique: les yeux et les oreilles de l'entreprise, Editions d'Organisation, 1995

- Moser Frédéric, Borry Marc, Intelligence Stratégique & espionnage économique : côtés pile et face de l 'information, Ed. Luc Pire & L 'Harmattan, parution prévue en février 2002