Stratégie de l'entreprise face aux risques d'attaques informatiques

Forum Annuel 2010 du CERTIST

« Incidents de sécurité :
responsabilités et moyens d'action de l'Entreprise »

CEIS

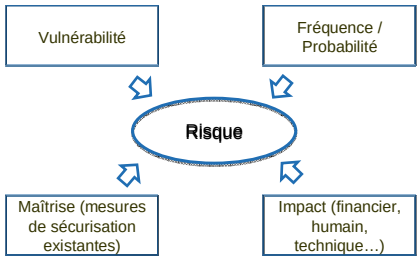
Introduction

- Une stratégie globale
  - Technique (veille technologique, tests d'intrusion…)
  - Humaine (sensibilisation, formation des utilisateurs)
  - Organisationnelle (Politique de Sécurité des Systèmes d'Information, CSIRT)
  - Juridique (gestion des logs)
- Des moyens
  - D'évaluation
  - De prévention
  - De gestion de crise
  - D'anticipation

Quelle stratégie ?

Les grands principes

- Nécessité de passer d'un mode réactif à un mode pro actif
  - Être préparé pour anticiper les risques
- Identifier et évaluer les risques afin de les gérer efficacement et « ne plus être surpris »
  - Etablir et surveiller ses profils de risques



Quelle stratégie ?

Les grands principes

- Accepter les nouveaux risques pour mieux les gérer
  - Ne pas interdire mais contrôler et accompagner :
    - Au niveau initialisation de projet : l'analyse de risque sur les spécifications métiers
    - Au niveau des déploiements de composants sensibles (ex PDA)
  - Être force de proposition dans l'innovation technologique
    - Virtualisation des environnements
    - Cloud Computing
- Gérer le passage d'un monde intra vers celui d'inter entreprises
  - Prendre en compte les risques liés à l'entreprise étendue
    - Extension horizontale avec échanges de données: ex les hubs de collaboration
    - Extension verticale avec perte du contrôle des données : ex :Cloud semi-public
  - Collaborer pour une sécurité globale
    - Dépendante du maillon le plus faible
    - Définir une gouvernance de sécurité

Quelle stratégie ?

La « pierre angulaire » de la sécurité

- La Politique de Sécurité des Systèmes d'Information
  - Un document fondamental de l'entreprise au niveau de la Direction Générale
  - Prise en compte les nouvelles menaces sur les actifs sensibles en particulier les postes de travail
  - Visibilité à l'intérieur de l'entreprise
  - Pour sa mise en œuvre, mise en place d'une organisation opérationnelle

Quels moyens ?

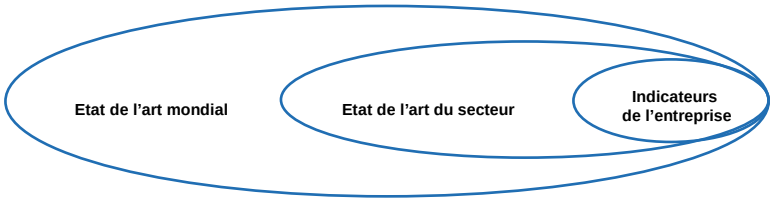
Des moyens d'évaluation

- Analyse de risques de type EBIOS 2010
  - Vision à 360°des enjeux de sécurité de l'information
  - Une démarche qui va aider à la mise en place d'un système de management ISO 27001
- Audits
  - De type organisationnel (ISO 27001/27002)
  - De type technique
    - Des tests d'intrusion sur les composants (ex dans les réseaux SCADA)
    - Des tests d'intrusion réseaux (inter et intranet)
    - Des tests de code (sur les sources de type freeware)

Quels moyens ?

Des moyens d'évaluation

- Mise en place de métriques standardisées (compatible ISO 27001/2)
  - Comparaison par rapport à d'autres entreprises (ex : le Club R2GS)
  - Introduction des objets métiers
  - Aboutissement : mise en place d'une approche SIEM



Intrusions et attaques			Dysfonctionnements	Usurpation d'identité interne	Vulnérabilité
Cybersquatting	Phishing	Défiguration de site web	Perte d'appareils mobiles non chiffrés	Utilisation illicite d'un accès après départ de l'entreprise	Mot de passe non conforme en solidité

Exemples d'indicateurs de sécurité opérationnels (Club R2GS)

Quels moyens ?

Des moyens de prévention

- L'utilisateur au centre de la sécurité de l'entreprise
  - Charte utilisateur
  - Modification du contrat de travail
  - Formations obligatoires et fréquentes
  - La sensibilisation
  - Bulletins d'alertes sur les menaces
- Mettre en place des indicateurs pour évaluer et ajuster
  - Un processus à long terme
  - Evaluation des formations
  - Des indicateurs quantitatifs (nombre de formations, pourcentage de réussite…) et qualitatifs (nombre de blocages de sessions, appels Help Desk…)

Quels moyens ?

Des moyens de gestion de crise

- Gérer la crise et l'après-crise
- PCA et PRA
- La question des traces informatiques : une protection juridique de l'entreprise
  - Pour dissuader les attaques internes comme externes
  - Pour réprimer : pour protéger ses droits, il faut démontrer le préjudice en présentant des preuves et les investissements financiers mis en œuvre dans la sécurité.
  - Pour prouver le respect de ses obligations : l'entreprise doit pouvoir attester qu'elle respecte bien les obligations légales auxquelles elle est soumise.
- L'entreprise doit faire preuve d'anticipation technique et juridique.
  - Elle doit se préparer à la nécessité de constituer des preuves.
    - Création de chartes et de politiques
    - Création de procédures de gestion des incidents
    - Création de séquestre des éléments de preuve.

Quels moyens ?

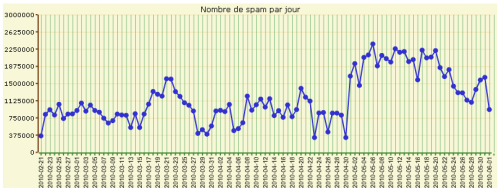
Des moyens d'anticipation

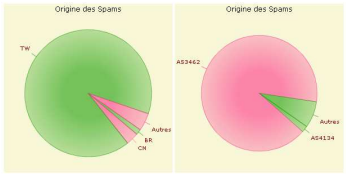
- Une veille sécurité à trois niveaux pour anticiper les menaces pesant sur le SI de l'entreprise
- Niveau 1 : une veille opérationnelle pour détecter les menaces quotidiennes
  - Surveillance des noms de domaine
    - cybersquatting,
    - typosquatting,
    - cybergriping.
  - Détection des actions malveillantes de phishing et de spams,
  - Détection des cyber attaques (DDOS, malwares, chevaux de Troie, virus, défigurations de sites Internet)
  - Surveillance des réseaux sociaux (fuite de données ?)

Quels moyens ?

Un exemple concret

- La menace du spam se poursuit en 2010 notamment sur les réseaux sociaux
  - Mise en place d'un observatoire du spam (CEIS)





Quels moyens ?

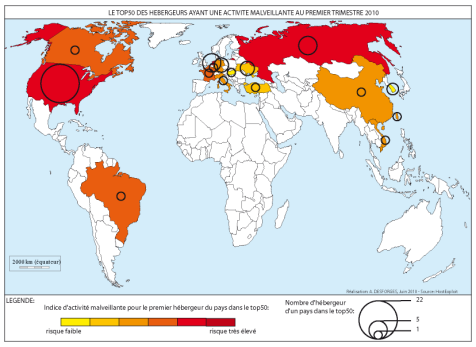
Des moyens d'anticipation

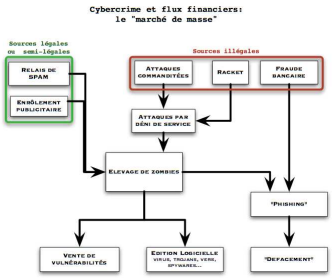
- Veille technologique : pour déceler les nouvelles tendances
  - Fraudes et cybercriminalité,
  - Vulnérabilités,
  - Intrusions informatique et incidents de sécurité,
  - Outils et techniques d'attaque,
  - Agenda des manifestations (salons, colloques, tables rondes; conférences…),
  - Publications (rapports, livres blancs, étude, analyses, présentations…),
  - Lois, réglementations, référentiels et normes,
  - Les nouveaux usages (Cloud Computing, mobilité…).

Quels moyens ?

Des moyens d'anticipation

- 3ème niveau : une veille stratégique
  - Objectif 1 : comprendre les mécanismes de la cybercriminalité



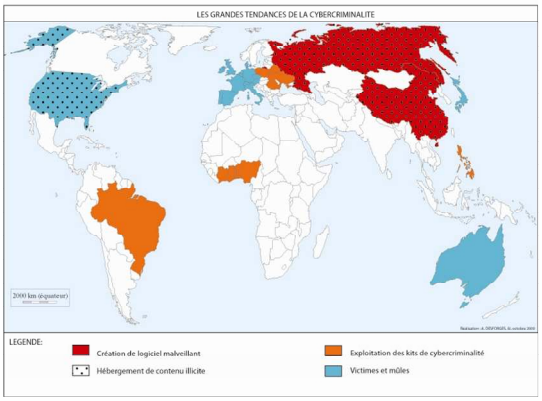


Source : étude d'HostExploit « Top 50 Bad Hosts and Networks »

Quels moyens ?

Des moyens d'anticipation

- 3ème niveau : une veille stratégique
  - Objectif 2 : évaluer le périmètre géographique des menaces



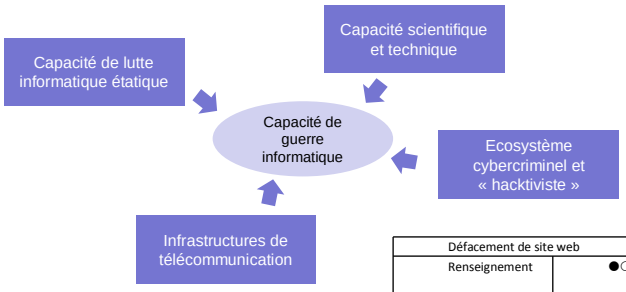
Une cybercriminalité à deux visages :

- Réseaux organisés, mafias traditionnelles
- Prolifération d'outils dits « clé en main »

Quels moyens ?

Des moyens d'anticipation

- 3ème niveau : une veille stratégique
  - Objectif 3 : appréhender le phénomène de « guerre informatique »



Défacement de site web	
Renseignement	●○○○○
Technique	●○○○○
Planification et organisation	●○○○○
Logistique	●○○○○
Investissements	●○○○○

Conclusion

- Une stratégie globale nécessaire pour répondre aux enjeux des cyber-menaces
- La PSSI : véritable « pierre angulaire » de la stratégie de sécurité de l'information
- Des moyens techniques, humains, organisationnels et juridiques à mettre en œuvre
  - Pour anticiper (veille opérationnelle, technologique et stratégique)
  - Pour évaluer les risques
  - Pour prévenir (formation / sensibilisation…)
  - Pour gérer la crise et les incidents