Sensibilisation à la sécurité informatique

Sébastien Delcroix <seb@cri74.org>

Attentes de son système d'information

- **Disponibilité**
- **Intégrité de ses données**
- **Confidentialité**

Qu'est-ce que la sécurité ?

- **Tous les éléments ou processus qui permettront à votre système d'information :**
  - D'être disponible
  - D'avoir des données intègres
  - De garantir la confidentialité

Les causes des problèmes 1/2

- **Aléas**
  - dysfonctionnement, erreurs
- **Attaques diverses**
  - Crackers
- **Les Malwares**
  - Spyware, Virus, Worm, Trojan, rootkit, exploit

Les causes des problèmes 2/2

- **Détournement frauduleux**
  - Phishing
- **Confidentialités**
  - VPN, Chiffrement, signature
- **Indésirables**
  - Spams, hoax

Démarche pour anticiper et résoudre les problèmes?

- Information et formation
- Appareils de protection
- Logiciels de protection
- Services

Informations et Formations

- **Connaissance des éléments de son SI**
  - Logiciels
  - Matériels
- **Connaissance des éléments perturbateurs**
  - Comment s'en protéger
  - Comment les éradiquer

Aléas de fonctionnement 1/3

- **Électrique**
  - Micro-coupures
  - Coupures longues
  - Surtension
- **=> Solutions :**
  - Onduleur
  - Groupe électrogène

Aléas de fonctionnement 2/3

- **Matériel**
  - Panne disque (le plus fréquent)
- **=> Solution :**
  - RAID
  - SAN/NAS

Aléas de fonctionnement 3/3

- **Humains**
  - Effacement / écrasement de fichiers
  - Ancienne version
- **Dégats**
  - incendie, inondation
- **=> Solution :**
  - Sauvegarde
  - Archivage
  - Doublement du stockage et des machines

Les attaques – pirates - leurs motivations – les risques

- **Accès aux données**
  - Pour vol ou destruction d'informations
    - Espionnage économique
    - Amusement
    - Revendications (politique ou non)
    - Vol de codes bancaires ou n° de cartes bancaires
- **Rebond**
  - Pirater d'autres sites
    - => Risque d'être inculpé à leur place
- **Planter un service**
  - Deny Of Service

Les attaques – Pirates – Comment ?

- **Connexion Internet quasi permanente**
  - Scans réguliers
  - Malwares
  - Tentatives d'attaques sur des failles de sécurité connues
  - Système mal configuré pour résister à une grosse charge
  - Système mal ou non sécurisé par défaut
    - Mot de passe inexistant
    - Failles connues non corrigées
  - 80% des attaques viennent de l'intérieur

Les attaques – Crackers – quelles solutions ?

- Pare-feu (Firewall), Routeur (Filtrage,NAT)
- Veille sécurité (se tenir informé)
- Système à jour
- Utilisation de protocoles sécurisés (mot de passe non visible)
- Système de détection d'intrusion (IDS)
- Pas d'accès physique aux machines (local sécurisé)

Les Malwares

- **Logiciels Malveillants**

Malware : virus

- **Programmes se propageant par de multiples supports**
- **Conséquences**
  - Destruction complète ou partielle des documents
  - Propagation vers d'autres SI (clients)
- **Solutions**
  - Avant tout : formation et information
  - Prévention / éradication : anti-virus

La vérité sur les anti-virus

- **Le tenir à jour quotidiennement**
- **Ne peut pas anticiper les nouveaux virus**
- **Ne filtrent pas tous les virus**
  - Anciens virus non filtrés
- **Meilleur anti-virus : LA VIGILANCE**
  - Formation et information
  - Filtrer les extensions suivantes :
    - bat, com, exe, pif, vb, lnk, scr, reg, chm, wsh, js, inf, shs, job, ini, shb, scp, scf, wsc, sct, dll

Malware : Worm & Trojan

- **Worm**
  - programme malveillant qui se propage de machine en machine
- **Trojan**
  - Programme malveillant permettant, entre autre, une intrusion à distance de votre machine

Malware : Spyware/Adware

- **Espionnage de votre machine**
- **Renvoie d'informations**
  - utilisation des informations à des fins commerciales ou autres !
- **Quelques chiffres (Misc N°17, p38, étude NCSA)**
  - 80% avec au moins 1 Spyware
  - en moyenne un PC héberge 93 spywares
  - record à 1059 spywares sur une machine
  - 90% des personnes interrogées ne savaient ce qu'était un spyware
- **exemple de logiciels installant des spywares**
  - Kazaa, codec DivX

Exploit et Rootkit

- **Exploit**
  - programme permettant d'exploiter une faille de sécurité
- **Rootkit**
  - Programme permettant de maintenir un accès à une machine déjà piratée (par un « exploit » par exemple)

Phishing

- Ingénierie sociale
- Mail indésirable
- Site web truqué
- Récupération données bancaires
- Détournement d'argent

Confidentialité / Intégrité de ses données

- **Problématique des informations de son SI et/ou circulant sur les réseaux**
- **Risques :**
  - Vol ou espionnage des données
  - Vol de code d'accès pour intrusion
  - Confidentialité de données sensibles en interne
  - Mobilité (données sensibles sur un PC portable)
  - Transport réseau facile d'accès (WiFi, Bluetooth)
  - Falsification d'information

Confidentialité / Intégrité – les solutions

- **Utilisation des protocoles sécurisés**
  - https, pop3s, imaps, etc.
- **VPN (Réseau Privé Virtuel)**
  - Relier deux réseaux de confiance via Internet et des protocoles chiffrés
- **Chiffrement des données**
  - Système de fichier chiffré (attention à la swap)
- **Validité d'un document**
  - garantir qu'un document n'a pas été falsifié pendant le transfert (signature électronique)

Les indésirables

- **Ces mails qui nous font perdre du temps**
  - SPAM
    - Publicité non sollicitée
    - Message souvent en anglais
    - => Solutions
      - Filtre anti-spam (n'est pas efficace à 100%)
  - HOAX
    - Rumeurs
    - Chaîne
    - => Solution : ne jamais renvoyer un hoax

Logiciels libres et sécurité

- **pas de sécurité par l'obscurité**
- **Code ouvert**
  - relecture et vérification du code par d'autres
- **utilisation d'algorithmes éprouvés**
- **Possibilité de faire éprouver ses programme par la communauté**
- **Meilleure réactivité sur les failles**
- **Attention, il faut quand même :**
  - mettre à jour son système
  - Être vigilant avec le téléchargement des packages (site de confiance, signature des packages)

100% Sécurisé : un mythe ?

- **La sécurité parfaite n'existe pas**
- **Pas simple**
  - Beaucoup d'acteurs et de facteurs
- **Anticipation impossible**

Ce qu'il faut faire au minimum

- Se former
- Être vigilant
- S'équiper des infrastructures, outils et logiciels essentiels (porte blindée, onduleur, sauvegarde, antivirus, firewall)
- Utiliser des logiciels sécurisés
- Éviter ceux qui sont mal réputés

Les coûts

- Vont dépendre du niveau de sécurité
- Ce n'est pas gratuit
- Il existe aussi des outils libres et peu chers
- Formation => investissement à long terme
- manque de souplesse dans l'utilisation
- Services fournis par les FAI, spécialistes (SSII/SSLL)

Conclusions

- Ce n'est pas simple
- Cela a un coût non négligeable
- Ce n'est jamais fiable à 100%
- par contre : C'est indispensable

Questions ?