



HERVÉ SCHAUER CONSULTANTS

Cabinet de Consultants en Sécurité Informatique depuis 1989

Spécialisé sur Unix, Windows, TCP/IP et Internet

# Sécurité des Postes Clients

**Table ronde CFSSI**

**Jeudi 29 mars 2007**

**Benjamin Arnault**

<Benjamin.Arnault@hsc.fr>

- Problématique sécurité du poste client
  - Enjeux, menaces et risques
- Sécurité système
  - Mesures de sécurité
- Solutions de protection
  - Systèmes de sécurité personnels
  - Contrôle d'intégrité réseau
- Automatisation de la sécurisation
- Perspectives

- Windows est utilisé *personnellement et professionnellement*
- **Omniprésent**
  - Intéressant pour les individus malveillants
- Développement d'Internet haut débit pour particuliers
  - croissance du nombre de cibles potentielles
- Des **menaces** qui planent aussi sur les systèmes d'information de l'entreprise

- Prise de conscience par le RSSI
  - Anciennement, la menace perçue était les *virus*
  - Evolution des **vers** pour exploiter des failles système automatiquement
  - Importance de la **mise à jour** des postes
- L'Internet « convivial » apporte avec ses nombreux avantages :
  - Logiciels espions
  - Des codes malveillants communicants (botnets)
  - Pourriels
  - Filoutage
  - De nouveaux besoins de communication : Données (légitimes?), Discussion, Voix ...
    - Apparition d'**infrastructures spontanées**

- Poste client
  - Système informatique mis à la disposition des utilisateurs
  - Poste fixe
  - Poste nomade (ordinateur portable), avec des **risques** supplémentaires
  - Système d'exploitation utilisé majoritairement : Windows XP
- Au delà de la sécurité du poste client : les **périphériques**
- Caractéristiques communes entre le poste client de l'entreprise et l'ordinateur personnel
  - Le poste de travail professionnel peut parfois être utilisé à des fins *personnelles*
    - Ex: consulter sa banque en ligne depuis son lieu de travail

- Vulnérabilités système
  - Exploitées de façon automatique via l'Internet, lorsqu'il s'agit de vulnérabilités exploitables à distance et de façon anonyme
  - Par la suite, exploitées par les vers
- Vulnérabilités du poste client
  - Tirer parti des vulnérabilités des applications installées communément
    - Applications intégrées, client VPN, fonctions coeur du système ...
- Vulnérabilités de l'infrastructure
  - Utilisateur à privilèges → Systèmes de protection moins efficaces
  - Contournement des mesures de filtrage
- Ingénierie sociale
  - Persuasion (filoutage, faux messages d'antivirus)

- Malwares
  - propagation : « toutes les portes d'entrée sont testées »
    - vulnérabilités
    - backdoors
    - comptes à mots de passe faibles
  - Vecteurs
    - Messagerie, services réseaux vulnérables, partages réseaux (SMB), messagerie instantanée, réseaux de pair à pair ...
  - Installation
    - Utilisent toutes les méthodes de Windows pour persister sur la machine
  - Fonctions
    - robots IRC
    - réseaux de robots pour attaquer (Dos, Spam, Phishing ...)

- Malwares
  - Modification de données : perte d'**intégrité**
  - Vol d'informations : perte de **confidentialité**
  - Déni de service : perte de **disponibilité**
- Attaques ciblées pour le profit
  - **pénétrer** dans un SI pour voler, modifier, entraver ...
- Vol
  - Oubli d'un ordinateur portable dans un taxi
  - Machine laissée sans surveillance dans un train
    - Perte de **disponibilité**
    - Potentielle perte de **confidentialité**

- Avant tout et avant d'installer tout système de sécurité
  - Travailler à la sécurisation du système Windows et examiner tout particulièrement les **services réseaux actifs**
  - Ne pas se connecter au système avec un **compte administrateur**
- Maintenir les systèmes à jour
  - Les *vulnérabilités système* sont un **risque majeur** pour le poste client
- L'antivirus est présenté comme un logiciel indispensable
  - Certainement **nécessaire** sur le poste client
  - Bien comprendre ce qu'il sait faire et ne pas faire
  - Attention à ne pas oublier qu'on accepte de mettre à jour *sans validation* un antivirus alors que les mises à jour de sécurité sont systématiquement validées

- « AAA » : Authentification, Autorisation, Audit
- Sécurité réseau
- Journalisation
- Maintenance

- Authentification
  - Mot de passe
  - Jeton
  - Biométrie
- Autorisation
  - Contrôle d'accès
    - Isolation des éléments système
    - Protection des données et programmes (chiffrement)
  - Principe de moindre privilège
    - Moins de **privilèges** → **Impact** moins important sur les actifs
- Audit
  - suivi des actions : accès et utilisation de privilèges

- De nombreux services sont **actifs** *par défaut*
- Plusieurs d'entre eux écoutent sur le réseau
  - Des **portes d'entrée** potentielles pour un attaquant
- Principe de sécurisation
  - **Minimisation** de la surface d'exposition réseau de la machine
    - *Identifier* les services réseau utilisés
    - *Désactiver* ceux qui ne sont pas utilisés
    - *Sécuriser* et restreindre les autres
- Protéger la machine avec un moyen de **filtrage IP**

- Deux sources d'information
  - Journaux EventLog
    - Vue globale du fonctionnement du système et de certaines applications
  - Journaux applicatifs
    - Informations précises sur les applications
- Utilisation
  - Assez peu connue en environnement Windows
  - De fait, **peu utilisée** pour des postes de travail (≠ serveurs)
- Intérêt
  - **Suivi** des machines
  - **Enquêtes** post incident

- La problématique de la **mise à jour** est omniprésente dans les solutions de sécurité
- De nouvelles **menaces** apparaissent *régulièrement*
- Implique la mise à jour du système qui est censé s'en protéger
- Deux types de mises à jour sont à considérer
  - Mises à jour des *logiciels*, pour protéger contre de nouvelles vulnérabilités
    - Mises à jour de Windows et des logiciels tierce partie
    - Mises à jour des *bases de signature* utilisées par des logiciels de sécurité
      - Antivirus, antispyware, IDS, IPS, ...
- Risque : **régression de service**

- Systèmes de sécurité personnels
- Contrôle d'intégrité réseau

- La sécurité doit être conçue en **couches successives** de protection.
- Sécuriser le poste client
  - Apporte une couche supplémentaire à la sécurité du SI.
- Les différentes couches de protection sur le poste client :
  - 1. La gestion des entrées et sorties de la machine
    - Le **pare-feu** (au niveau des interfaces réseau)
    - Le **contrôleur de média amovible**
  - 2. La contrôle des entrées du système (ouverture de fichier)
    - L'**anti-virus** et l'**anti-spyware**
  - 3. La surveillance constante des processus et de leurs interactions
    - Le **système de détection/prévention d'intrusion**

- 802.1x
  - **Authentification et autorisation** pour l'accès au réseau
  - Au niveau liaison de données (2)
  - Utilise une extension du protocole **EAP** (Extensible Auth. Protocol)
    - Transport au dessus du protocole de liaison **EAPoL** (EAP over LAN)
  - Deux types de ports
    - Authentification
    - Service : ouvert après authentification
  - Nécessite
    - La compatibilité logicielle du *système d'exploitation*
    - La compatibilité protocolaire des *équipements réseau*
    - Un *serveur d'authentification* (ex : RADIUS)
  - Lourd à mettre en place ... mais adapté au Wi-Fi avec WPA/WPA2

- Quarantaine
  - *Ce n'est pas une solution de **sécurité** !*
  - Permet de connaître « l'état de santé » d'une machine
    - Mises à jour de sécurité
    - Solutions de sécurité : présentes ? à jour ?
    - Client d'accès distant convenablement configuré
    - Présence de programmes interdits
  - Plusieurs solutions **interopérables** : NAP (Microsoft) et NAC (Cisco)
  - Risque
    - Se jouer du contrôle en fournissant un **bulletin de santé falsifié** !

- Indispensable en environnement d'entreprise
- Système
  - Group Policy Objects
    - Déployer des ensembles d'options de sécurité sur un périmètre large
  - WSUS, SMS, MOM
    - Proposer les mises à jour de sécurité
    - Suivre un parc de machines
  - Solution tierces
- Solutions de protection et contrôle d'intégrité réseau
  - Serveurs applicatifs d'administration adhoc
    - Surveillance
    - Mise à jour des clients

- Les menaces ont **évolué**
  - Le challenge : For fun ...
  - La phrase prémonitoire : « *For fun and profit !* »
  - Aujourd'hui : For *fun* and **PROFIT**
- La problématique du **réseau domestique**
  - Nouveaux équipements : domotique, électroménager, jeu ...
  - Infections de la part d'autres équipements du réseau
  - Nécessité d'une **sécurité réseau chez soi**
- La prise en compte de la sécurité
  - dans le développement :  **systèmes d'exploitation** (Windows Vista)
  - par les directions : **gestion de la sécurité de l'information**

**Merci de votre attention**