

La sécurité des accès grand public

Cédric Blancher

blancher@cartel-securite.fr



Cartel Sécurité

Salon Vitré On Line
25-27 octobre 2002

Plan

- **1. Introduction**
- **2. Les risques spécifiques**
- **3. Les bonnes habitudes**
- **4. Les outils disponibles**
- **5. Les sites sécurisés**

Partie 1 - Introduction

Internet...

- **Le réseau des réseaux**
- **De nombreux services à buts divers**
 - **Communication (Émail)**
 - **Espaces de publications (Web)**
 - **Espaces de discussion (Chat, forum)**
 - **Etc.**

Introduction...

La sécurité...

- Contrôler les données reçues
- Contrôler les données émises

☹ **Vaste programme !**

Introduction...

La sécurité est difficile à obtenir

- **Domaine compliqué**
- **Mauvais réflexes**
- **Outils inadaptés**
- **Détournement médiatique**

Introduction...

Les accès grand public

- Ligne téléphonique
- Câble & ADSL

Utilisation cliente d'Internet, serveur rares

➔ Problématique particulière

Partie 2 – Les risques

- **Virus et assimilés**
- **Fuite d'informations**
- **Prise de contrôle**
- **Espionnage et détournement de flux**
- **Attaque des logiciels**

Les risques...

La menace virale...

- Programmes mal intentionnés
 - ➔ Se répliquent
 - ➔ Peuvent installer des outils
 - ➔ Peuvent transmettre des données

Les risques...

Les fuites d'informations

- **Des sites ou des programmes qui collectent des informations**

- ➔ **Documents**

- ➔ **Identité**

- ➔ **Habitudes**

- ➔ **Etc.**

Les risques...

Prise de contrôle

- **Des outils qui permettent à un pirate de contrôler votre ordinateur**
 - ➔ **Espionnage**
 - ➔ **Vol d'identité**
 - ➔ **Etc.**

Les risques...

Attaque des flux réseau

- **Détournement de connexions**
 - ➔ **Redirection vers des sites pirate**
 - ➔ **Espionnage**
 - ➔ **Modification des données**

Risques...

Attaque des logiciels

- Logiciels serveurs
- Logiciels clients
- Fonctionnalités des systèmes
(partage de fichiers)

➔ Actions détournées

Partie 3 – Les bonnes habitudes

- L'utilisateur est l'ennemi numéro 1 de la sécurité de son accès
 - MAIS c'est aussi son allié le plus efficace !
- ➔ Un paradoxe à résoudre...

Les bonnes habitudes

Contrôler ses logiciels

- Source des programmes
- Suivre les versions
- Utilité des logiciels ou de leurs fonctionnalités

Les bonnes habitudes

Bien gérer ses communications

- **Identifier ses interlocuteurs**
- **Ne pas donner d'informations personnelles inutilement**
- **Ne pas répondre au spam**
- **Ne pas ouvrir les documents inconnus**

Les bonnes habitudes

Utiliser des outils de sécurité

- Un environnement sécurisable
- Un logiciel antivirus
- Un pare-feu (firewall) personnel
- D'autres outils divers...

Partie 4 – Les outils de sécurité

Les alliés indispensables

Ne dispensent pas d'une bonne
« hygiène » de navigation

✘ Ce ne sont pas des solutions
universelles et infaillibles !!!

Les outils de sécurité

Les environnements...

- **Le système d'exploitation est la brique de base**
- **Il doit prendre en compte la sécurité**
- ➔ **Les OS grand public ne vont pas**
- ➔ **La sécurisation demande de s'impliquer et d'apprendre...**

Les outils de sécurité

Les logiciels antivirus

- Contre les virus et assimilés
- Basés sur des bases de signatures
- ➔ Doivent tourner en tâche de fond
- ➔ Doivent être mis à jour

Les outils de sécurité

Des logiciels antivirus

- **Antivir** : <http://www.hbedv.com/>
 - Gratuit
- **Kasperski AV** : <http://www.kav.ch/>
 - Réputé
- **Norton AV, McAfee**
 - Souvent installés d'origine

Les outils de sécurité

Les firewalls personnels

- **Filtrent les applications**
 - ➔ **Luttent contre les logiciels espion**
 - ➔ **Luttent contre les accès furtifs**
 - ➔ **Limitent l'accès aux serveurs**
 - ➔ **« Dissimulent » l'ordinateur**

Les outils de sécurité

Des logiciels pare-feu

- **Kerio PF** : <http://www.kerio.com/>
 - Gratuit et très complet
- **ZoneAlarm** : <http://www.zonelabs.com/>
 - Gratuit et simple
- **Outpost** : <http://www.agnitum.com/>
 - Gratuit et efficace

Les outils

Des outils divers

- **PGP : chiffrement et signature**
 - <http://www.pgpi.org/>
- **AdAware : chasse les « spywares »**
 - <http://www.lavasoft.de/>
- **Verrouillage et contrôle de contenu**
- **Attention aux faux logiciels de sécurité !!!**

Partie 5 – Les sites « sécurisés »

Les comptes Émail, le commerce électronique, les sites bancaires...

- **Authentification des parties**
- **Confidentialité des échanges**

Les sites « sécurisés »

Utilisation de SSL

- SSL permet de s'assurer de l'identité du site
- SSL permet le chiffrement de la session

Les sites « sécurisés »

SSL ne concerne que la connexion entre le client et le serveur

- **Ce n'est pas un garant de la sécurité du serveur**
- **Ce n'est pas un garant des bonnes intentions du serveur**

Le commerce électronique

Les réflexes :

- **Bien choisir son site, même si c'est difficile**
- **Bien vérifier le certificat du site**
- **Ne jamais laisser de coordonnées bancaires au site**

Le commerce électronique

Les risques sont présents mais exagérés

- **Vol de coordonnées bancaires (CB)**
 - ➔ **Ça peut arriver**
 - ➔ **Bien vérifier ses relevés de CB**
 - ➔ **Tout paiement par CB sans code est contestable !**

Les sites bancaires

Risque plus important

- **Accès à des données et des opérations bancaires limitées**
- ➔ **Bien gérer les possibilités offertes par cet accès**

Les comptes Émail

**Un atteinte certaine à votre privée,
mais des conséquences très
limitées.**

- **Lecture de courrier**
- **Usurpation d'identité**

Deux attaques classiques

- **Attaque de l'homme du milieu (Man in the Middle attack)**
 - On détourne l'internaute vers un relais
 - On observe ce qu'il fait
- ➔ **Bien vérifier le certificat du site !**
- ➔ **Mettre à jour son navigateur 😊**

Deux attaques classiques

- **Injection de scripts intersites (Cross Site Scripting ou XSS)**
 - On envoie l'internaute vers un site valide, mais avec des scripts de redirection
- ➔ **Regarder où on clique !**

Des questions ?



Contacts...

- **Cédric Blancher**

- blancher@cartel-securite.fr

- **Cartel Sécurité**

- <http://www.cartel-securite.fr/>

- **Vitré On Line**

- <http://www.mairie-vitre.fr/vitreonline/index.html>