



Enjeux et perspectives en sécurité



Capital-IT
13 avril 2005

Hervé Schauer
<Herve.Schauer@hsc.fr>

- Société de conseil en sécurité informatique depuis 1989
- Prestations intellectuelles en toute indépendance
 - Pas de distribution, ni intégration, ni infogérance, ni régie, ni investisseurs
- Prestations : conseil, études, audits, tests d'intrusion, formations
- Domaines d'expertise
 - Sécurité Windows/Unix/embarqué
 - Sécurité des applications
 - Sécurité des réseaux
 - TCP/IP, PABX, réseaux opérateurs, réseaux avionique, ...
 - Organisation de la sécurité
- Etude de nombreux projets ou sociétés en sécurité

**Les transparents sont
disponibles sur
www.hsc.fr**

- Chiffres ?
- Opportunités du marché de la sécurité
 - Edition de logiciels, services, ...
 - Protection du PC ou poste de travail
 - Protection des autres équipements
 - Mobilité et nomadisme
 - HTTP/HTTPS
 - Fusion internet et telecom
 - Gestion des données de la sécurité
- Autres sujets
- Conclusion

- Livre blanc des Assises de la Sécurité
 - Enquête auprès de RSSI
- Indicateurs sécurité dans chaque n° de CSO
- Idem dans toute la presse : nombreuses enquêtes, nombreux chiffres de cabinet d'analyse
- Chiffres du Clusif

- Pertinence de ces chiffres ?

- Arrivée depuis 2004 de la malveillance sur internet
 - La même que dans la société en général

- Edition de logiciels
 - Logiciel vendu ==> logiciel loué à l'usage
 - Logiciel à installer ==> logiciel en appliance
 - Des opportunités
 - Protection du PC
 - Protection des autres équipements
 - Mobilité et nomadisme
 - HTTP/HTTPS
 - Fusion internet et telecom
- ==> **L'édition de logiciels concentre les opportunités à forte marge**

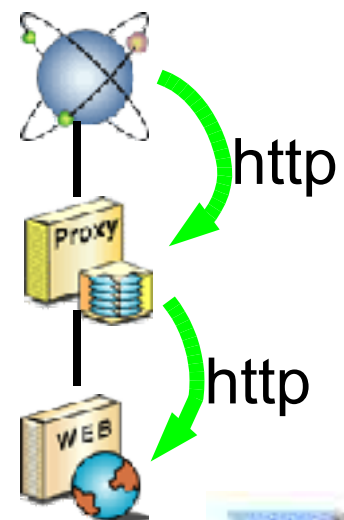
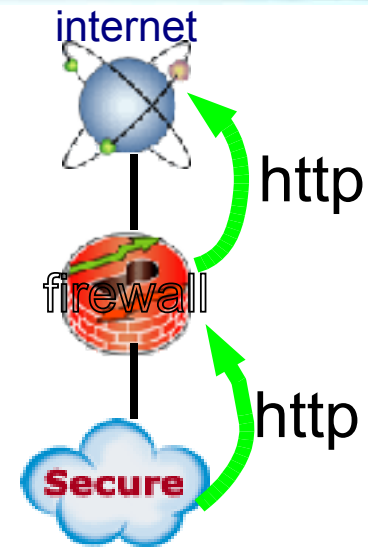
- Edition de supports pédagogiques
 - Sensibilisation
 - Enseignement à distance
- Services
 - Externalisation
 - Infogérance de la sécurité
 - Opérateurs d'infrastructures et marchés de niches
 - Service aux opérateurs
 - Formation et sensibilisation
 - Sécurité physique
- Produits techniques à forte valeur ajoutée pas toujours adaptés à la vente indirecte

- Virus, *firewall* personnel
- Contrôle de l'usage des périphériques amovibles
- Logiciels espions et malveillants (*spyware*, *malware*), renifleurs de clavier (*keyloggers*), robots
- **⇒ La protection du poste de travail demeure une bonne opportunité**
- Inconnue : jusqu'où ira Microsoft dans le système de base
 - Exemple : chiffrement du disque dur

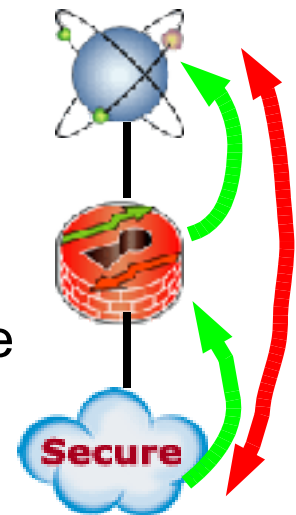
- Assistants personnels, téléphones portables, voitures, ...
 - Chiffrement des données
 - PalmOS, Symbian, WindowsCE, ...
 - Virus / vers preuves de concepts
 - Vulnérabilités réelles
 - Modèle économique qui repose plus sur l'opérateur que pour le PC
- **⇒ Opportunité peut-être plus coté infrastructure qu'utilisateur final**

- **Une difficulté en entreprise**
- **Ordinateur portable, assistant personnel, téléphone, ...**
 - Une organisation, un service de support, des procédures d'alerte, un inventaire temps réel du parc connecté
 - Une authentification de l'employé et une connexion au SI par tunnel chiffré
 - Contrôle d'intégrité et mise en quarantaine avant la reconnexion au réseau d'entreprise
- Une politique de protection locale du mobile ou nomade lui-même
 - Firewall + anti-virus + anti-spyware + ... gérés de manière centralisés
 - Chiffrement des données (indispensable contre le vol)
 - Maintien à niveau des moyens de protection lorsque le nomade est à l'extérieur
- **⇒ Opportunités dans la cohérence globale**

- Le protocole de base sur Internet est HTTP/HTTPS
 - HTTP et HTTPS sont les protocoles autorisés dans les entreprises avec le DNS par le firewall entre le réseau privé à protéger et l'Internet
 - HTTP : protocole du web
 - HTTPS : version chiffrée de HTTP
 - DNS : correspondance entre les noms (www.hsc.fr) et les adresses IP (217.174.211.25)
 - La politique de sécurité appliquée par le firewall IP est contournée par la ré-encapsulation de tous les trafics dans les protocoles HTTP et HTTPS
- Offre déjà développée pour les *firewalls* ou *proxy* protégeant les serveurs web de l'internaute



- Le *firewall* doit donc filtrer les logiciels de contournement potentiel de sa politique de sécurité par encapsulation dans HTTP/HTTPS
 - Logiciels réencapsulant volontairement
 - Microsoft avec RPC over HTTPS, Outlook 2003, etc
 - VPN-SSL, ssltunnel, stunnel, http-tunnel, etc
 - Courrielweb (*Webmail*), systèmes d'EDI, XML
 - Logiciels de messagerie instantanée, de messagerie et partage d'agenda
 - AOL, MSN, Blackberry, etc
 - Logiciels basés sur les *Web Services*
 - Logiciels poste à poste (*P2P:Peer-toPeer*)
 - Skype
- **⇒ Le firewall HTTP demeure une bonne opportunité**



- Une forme de firewall HTTPS en sortie est possible
 - La type de trafic même chiffré peut se reconnaître
 - SSL VPN connection multiplexing techniques
 - <http://www.hsc.fr/ressources/presentations/upperside05-fw/>
- Filtrage d'URL
 - Utile à la lutte contre les *spywares* en entreprise
- Innovations encore possibles

- Les **télécommunications** et l'**Internet** ne font qu'un
 - Le PABX classique est un ordinateur Unix qui interroge l'annuaire d'entreprise
 - La télémaintenance par liaison téléphonique en PPP ne sert qu'à contourner le *firewall* sur les liaisons IP
 - SAN
 - Le photocopieur est un PC avec scanner/imprimante sur le réseau d'entreprise et télémaintenu par une ligne téléphonique
 - Les liaisons séries des immeubles intelligents passent aussi à IP
 - RS232 devient Telnet sans authentification
 - Les protocoles propriétaires (LonTalk, BACnet) sont ré-encapsulés sur IP
 - Voix sur IP / Téléphonie sur IP / GSM sur IP ...
 - Le PABX ou Centrex remplace toutes les strates de *firewalls* IP
- **⇒ Opportunité pour un *firewall* global télécoms + internet**

- Centralisation et analyse des journaux (SIM)
- Génération d'alarmes, d'alertes, tableaux de bord
- Consolidation et archivage
- Visualisation pour les exploitants
- Détection d'intrusion (IDS), prévention des intrusions (IPS)
- Déjà beaucoup d'offres existantes
 - Dont une offre de logiciels libres
- Repose sur les individus
 - Beaucoup de déception

- Réseaux sans fil
 - La sécurité est intégrée dans l'infrastructure
- Voix sur IP / Téléphonie sur IP
 - La sécurité est en cours de normalisation et sera à terme intégrée à l'infrastructure
- Infrastructures à clés publiques, biométrie
- Lutte contre le spam
 - Offre liée à la lutte anti-virus + logiciel libre
- Gestion des droits des oeuvres numériques

- Panorama non-exhaustif
- Toujours une bonne opportunité pour des jeunes pousses
- Rappel : la sécurité n'est qu'un *nice to have*, jamais un *must*
 - Toujours un équilibre entre une prise de risque et une réduction du risque
 - Donc sensible à l'économie en général

Questions ?

Herve.Schauer@hsc.fr
www.hsc.fr

- Sur **www.hsc.fr** vous trouverez des présentations sur
 - Infogérance en sécurité
 - Sécurité des réseaux sans-fil
 - Sécurité des SAN
 - Sécurité des bases de données
 - SPAM
 - BS7799
 - etc
- Sur **www.hsc-news.com** vous pourrez vous abonner à la **newsletter HSC**