



HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis
1989
Spécialisé sur Unix, Windows, TCP/IP et Internet

Menaces et sécurité préventive



Matinales Sécurité Informatique
18 mai 2006

Hervé Schauer
<Herve.Schauer@hsc.fr>

- Menaces
- Infrastructures spontanées
- Mobilité
- Voix sur IP
- Sécurité préventive
- Firewall, IDS et IPS
- Solutions
- Conclusion

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

- Sur la protection périmétrique
 - Infrastructures spontanées
 - Mobilité
 - Difficulté à comprendre où se situe la limite du périmètre
- Globalement
 - Voix sur IP

- Ensemble de matériels, logiciels, services, ...
- Utilisateur a un besoin →
- Service informatique
- Projet
- Maîtrise d'ouvrage
- Maîtrise d'oeuvre
- Contrats de service
- Contrôle qualité
- Sécurité ←
- Besoin de l'utilisateur est satisfait

- Ensemble de matériels, logiciels, services, ...
- Utilisateur a un besoin
- Télécharge ou achète lui-même



- Besoin de l'utilisateur est satisfait

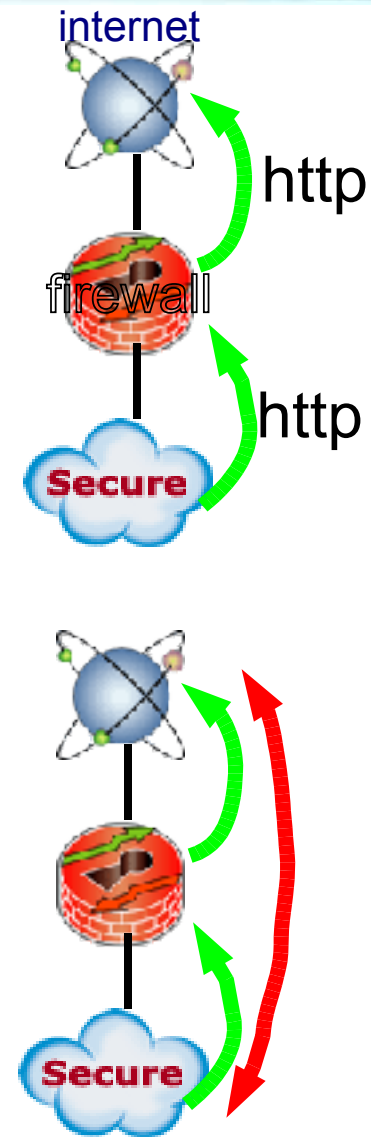
Spontaneous infrastructure

Click-and-run applications

- Service informatique inutile
- Pas de projet
- Pas de maîtrise d'ouvrage
- Pas de maîtrise d'oeuvre
- Pas de contrats de service
- Pas de contrôle
- Pas connaissance du besoin
- **Sécurité ?**

- Infrastructure qui apparaît de manière spontanée
- Par opposition aux infrastructures qui sont mises en place par la direction des systèmes d'information
- Principaux vecteurs
 - Services disponibles sur internet
 - Courrielweb, messageries instantanées
 - Téléchargement de logiciels sur internet
 - Logiciels espions (*spywares*)
 - Softphone
 - Achats de matériel
 - Par l'individu : téléphone, assistant personnel, lecture à distance de BAL
 - Par son département métier ou l'achat de consommables

- Création d'un **réseau virtuel** poste à poste
 - Dialogues poste à poste (*peer to peer*)
- **Contournement de la protection périmétrique**
 - Sur le poste de travail si pas de contrôle central avec des agents performants sur chaque poste
 - USB, bluetooth, SD-Card, etc
 - Sur le périmètre réseau par encapsulation dans HTTP ou HTTPS
 - Pas de limite aux ré-encapsulations avec les *firewalls* n'incluant pas de filtrage dans HTTP
- Utilisation d'un serveur sur internet
- **Pas de contrat** autre que le clic de souris



- X25 et réseaux privés : contrat de bout en bout
- Accès internet : contrat sur son extrémité
- Infogérance : contrat de service
 - Sécurité
 - Répartition des rôles et responsabilités
- Réseaux spontanés : pas de contrat
 - Infogérance cachée



<http://dona.ferentes.free.fr/>
reproduit avec autorisation

- Infrastructures spontanées : adaptées au grand public
 - Environnements sans gestion, sans contrôles et sans besoins spécifiques
 - Infogérance sans contrat de service
- Infrastructures spontanées : inadaptées aux entreprises
- Pourtant utilisées en entreprise :
 - WebEx, InterWise, Genesys, MeetingOne, etc.
 - Softphones : Skype, etc

- Il y a toujours :
- Un espace dont je suis responsable
 - Le système d'information (SI) de l'entreprise
- Un espace dont je ne suis pas responsable
 - Le reste du monde
- Il existe et existera toujours un **périmètre** entre les deux
- J'applique la **politique de sécurité** de mon entreprise dans le SI et sur ce **périmètre**

- PDA, téléphones, lecteurs MP3, etc sont des PC
- PC utilisés par l'employé achetés personnellement
- Données sur ces outils de la mobilité sont les données de l'entreprise
 - La base des clients est dans l'ordinateur portable, dans l'assistant personnel, dans le téléphone portable, dans la clé USB, ...
- L'usage des outils de la mobilité est au moins en partie professionnel

- Pas équivalent à la téléphonie classique
 - Signalisation/contrôle et transport de la voix sur le même réseau IP
 - Perte de la localisation géographique de l'appelant
- Pas la sécurité à laquelle les utilisateurs étaient habitués
 - Pas d'authentification mutuelle entre les parties, peu de contrôles d'intégrité des flux, pas de chiffrement
 - → Intrusion, écoute, usurpation d'identité, rejeu, surfacturation, dénis de service
- Terminaux très fragiles
 - Exemple téléphone VoIP sur WiFi Cisco 7920
 - port 7785 Vxworks wdbRPC ouvert
 - SNMP Read/Write
 - Réponse de Cisco : les ports ne peuvent pas être désactivés, la communauté SNMP ne pas être changée : tout est codé en dur dans le téléphone...

- Menaces et sécurité préventive
 - *threats and preemptive security*
 - *preemptive* -> préventif
 - préventif --> *preventive, preemptive*
- Vocabulaire courant : "prévention d'intrusion"
 - *Firewall, IDS, IPS*

- Filtrage IP
 - *firewall*
 - Contrôle d'accès réseau
 - Proactif : le paquet passe où le paquet est bloqué
 - Application de la politique de sécurité de l'organisme

- Détection d'intrusion (NIDS)
 - Passif : le paquet est passé mais finalement il n'aurait pas dû, il est malveillant
 - Faux positifs : un paquet vu comme malveillant qui est tout à fait légitime
 - Faux négatif : un paquet vu comme légitime qui est malveillant

- Prévention d'intrusion (NIPS)
 - Combiner l'analyse approfondie de la détection d'intrusion avec la capacité de bloquer du *firewall*
 - Actif : certains paquets sont passés, mais pas les suivants :
 - Limitation de bande passante
 - TCP Reset / ICMP Unreachable
 - Toujours des risques de faux positifs / faux négatifs

- Mesure de sécurité, ou protection
 - Action
 - Diminue le risque à un niveau acceptable
- Action préventive **IS 19011:2002 5.5.a)**
 - Action visant à éliminer une situation indésirable potentielle
 - Agit en amont de l'incident
- Action corrective
 - Action visant à éliminer une situation indésirable détectée
 - Agit en aval de l'incident

- Actions préventives ?
- Donc réfléchir sans attendre l'incident !
 - Identifier se qui compte pour le chef d'entreprise
 - Réaliser une analyse de risque sur ce qui compte
 - Appliquer des mesures de sécurité
 - Avec un rapport qualité/prix réaliste
 - Afin de réduire les risques à un niveau acceptable

- Sensibilisation, formation, explications
- Formalisation contractuelle des infogérances obligatoire
- Mention explicite des infrastructures spontanées dans les documents d'application de la politique de sécurité
- Filtrage des protocoles sur la protection périmétrique
- Interdiction sur les PC des logiciels qui ne sont pas explicitement autorisés

- Ou... considérer les PC comme étant hors du SI d'entreprise

- Choix à faire
- PC (PC, PDA, téléphone, etc) sous la maîtrise de l'entreprise
 - Configuration pré-déterminée et gestion centralisée
 - Firewall personnel, anti-virus, système de mise en quarantaine ...
 - Application des correctifs , mise à jour de l'anti-virus
 - Chiffrement de la mémoire de masse
 - Sauvegarde automatique
- PC abandonné par l'entreprise
 - Identique au PC personnel à la maison
 - Tunnel chiffré et authentification forte pour accéder au SI d'entreprise
 - Accès au SI limité et contrôlé en conséquence

- Calcul du retour sur investissement
 - Mettre à jour son PABX apporte les mêmes service avec ou sans VoIP
 - Intégrer les coûts de la VoIP
 - Aucun client HSC n'a survécu sans VLAN, avant même les considérations de sécurité
 - Service téléphonique doit savoir dans quel pièce et sur quelle prise est chaque numéro de téléphone
 - N° de téléphone, @MAC, @IP et n° de prise Ethernet sont liés
 - Coûts de cablage
 - Poste téléphonique IP => prise ethernet supplémentaire
 - Plusieurs clients ont eu des difficultés avec le PC connecté sur le téléphone et le téléphone dans la prise Ethernet du PC
 - Cablage de prises spécifiques avec le courant électrique sur le cable Ethernet (PoE)
 - Onduleurs supplémentaires et spécifiques

- Intégrer les coûts de la VoIP
 - Services du réseau informatique deviennent des services **critiques**
 - DHCP
 - DNS
 - Commutateurs
 - ...
 - Mise en oeuvre de la haute-disponibilité devenue obligatoire
 - Exploitation 24/7
- Intégrer la dégradation du service due à la VoIP
 - Taux d'indisponibilité téléphonie classique : 5 à 6 minutes d'interruption par an, 99,99886 %
- Support téléphonique hors-service
 - « Quand le réseau est panne il n'y a plus non plus de téléphone comme ça on est dérangé que par ceux qui utilisent leur mobile »
 - Téléphone : principal système d'appel au secours pour la sécurité des personnes


- Infrastructures spontanées → **danger**
- Mobilité → **difficulté de maîtrise**
- Voix sur IP → **danger**
- Reprenez votre politique de sécurité
- Analysez explicitement les menaces, vulnérabilités, risques et impacts
- De manière préventive, avant les incidents !

Questions ?

Herve.Schauer@hsc.fr

www.hsc.fr

- **Formation ISO27001 Lead Auditor :**
 - Certification ISO27001 Lead Auditor par **LSTI**
 - <http://www.hsc.fr/services/formations/>

A small version of the HSC logo is placed to the left of the text.

Toulouse : 5-9 juin
Paris : 19-23 juin
Genève : 28 août-1sep