



HERVÉ SCHAUER CONSULTANTS

Cabinet de Consultants en Sécurité Informatique depuis 1989

Spécialisé sur Unix, Windows, TCP/IP et Internet

# Gérer les nouvelles formes d'insécurité informatique

Conférence



Les 7 leviers d'excellence de la DSI 2004-2005

**Comundi / Reed**

**30 juin 2004**

**Hervé Schauer**

<Herve.Schauer@hsc.fr>

- x HSC
- x Contexte
- x Quels enjeux en sécurité
- x Progiciel
- x Vers et virus
- x Infogérance/Télemaintenance
- x Périmètre
- x Applications
- x Conclusion

- x Société de conseil en sécurité informatique depuis 1989
- x Prestations intellectuelles en toute indépendance
  - x Pas de distribution, ni intégration, ni infogérance, ni investisseurs
- x Prestations : conseil, études, audit, tests d'intrusion, formations
- x Domaines d'expertise
  - x Sécurité Windows/Unix/embarqué
  - x Sécurité des applications
  - x Sécurité des réseaux
    - x TCP/IP, PABX, réseaux opérateurs, réseaux avionique, ...
  - x BS7799
- x Principalement contacté par les responsables sécurité
  - x Ou collaborateurs ou assimilés

- x Contexte économique souvent difficile
- x Le DSI doit
  - x Gérer le quotidien et accroître la productivité interne
  - x Supporter une foule d'anciennes applications et intégrer des applications nouvelles
  - x Ouvrir sans arrêt le système d'information sur l'extérieur sans nuire à celui-ci en interne
  - x Répondre aux exigences des métiers en matière de nouvelles technologies et d'hétérogénéité et développer la cohérence du parc informatique
  - x Se justifier économiquement
    - x Réduire les coûts, calculer des ROI, se transformer en centre de service, ...
- x ⇒ **La sécurité n'est pas toujours une priorité**

- x Virus et vers
- x Spam
- x Correctifs de sécurité et des mises à jour
- x Denis de services et chantages aux dénis de service
- x Maitrise du périmètre et réseaux sans fil
- x Téléphonie sur IP
- x Intégration des ordinateurs nomades et assistants personnels
- x Infogérance
- x Migration vers des solutions d'identification/authentification universelles
- x Journalisation et tableaux de bords en sécurité
- x Télémaintenance

- x Au début et pendant longtemps, pour un éditeur de logiciel
  - La sécurité il faut en parler le moins possible et ne pas en faire*
- x Puis sur la pression des utilisateurs, certains éditeurs ont adopté un nouveau discours :
  - La sécurité il faut en parler le plus possible et en faire le moins possible*
- x Et maintenant le discours technico-marketing est désormais
  - La sécurité il faut en faire pour soi et faire croire qu'elle est pour le client*
- x Il n'y a pas de notion d'assurance qualité dans le progiciel
  - x Le responsable de la défaillance d'un logiciel est son utilisateur, pas son éditeur

- x Demander un système qui répond a ses besoins et ne pas accepter un système qui répond aux besoins du fournisseur
- x Reprendre ses contrats, engager la responsabilité de l'éditeur
- x Ne pas oublier que dans le cas de sécurité et la supervision, elle se fait par de l'organisation, pas par un logiciel structurant avec un ROI mirobolant
- x Diversifier les systèmes d'exploitation et les logiciels de base : bureautique, messagerie, butineur
- x Ne pas oublier que le droit de propriété est supprimé, il est remplacé par un droit d'usage à la demande

- x Le contrôle d'accès obligatoire ne protège pas du code malveillant
- x Les vers montrent les limites des infrastructures
- x Les principaux logiciels comportent un grand nombre de failles
- x Slammer
  - x Serveurs MS-SQL
  - x Duplication rapide par diffusion
- x Sobig
  - x Envoi de messages en masse par un logiciel de messagerie
  - x Intérêt financier : le SPAM ?
- x Les vers s'attaquent plutôt aux logiciels très répandus

- x Lancé le 11 août 2003
- x Utilise une faille dans une partie ancienne de Windows dont le correctif a été publié un mois avant (16 juillet 2003)
- x Réplication par des ports de communication normalement fermés par les *firewalls*
- x Volontairement très lent, environ 2000 ordinateurs par heure
- x Ciblait à terme un déni de service que un serveur : [www.windowsupdate.com](http://www.windowsupdate.com) qui a pu être facilement évité
- x A provoqué la mise à jour de la majorité des postes de travail W2K & WXP
- x Dupliqué sur des réseaux non-connecté à l'Internet ou protégés de l'Internet via les postes nomades
  - x Premier ver mettant clairement en avant ce type de risque

- x Perte de temps par les équipes bureautique et sécurité
  - x A pris les utilisateurs durant les vacances
- x Un des éléments de la cascade de pannes dans la coupure électrique aux USA ?
- x Un des éléments du défaut d'information au ministère de la santé lors de la canicule ?
- x A permis d'éviter un incident beaucoup plus dramatique
- x A permis à plusieurs équipes de se pencher sur la partie de Windows incriminée et d'en découvrir de nombreuses autres failles similaires
  - x De nouveaux correctifs ont été publiés en conséquence
- x A qui a profité Blaster ?

- x Très peu de vers sont développés par rapport aux possibilités
  - x Beaucoup de failles logiciel dans les logiciels très répandus
  - x Une population de plus en plus large capable d'exploiter les failles
- x Pas ou peu de vers exploitent les nouveaux vecteurs de propagation :
  - x Systèmes de messagerie instantanée
  - x Logiciels poste à poste (*peer-to-peer*)
  - x Assistants personnels
  - x Téléphones portables
- x Pas ou peu de vers s'attaquant à une cible précise comme un ensemble d'organismes
  - x Si uniquement un organisme est visé, quel sera le support des éditeurs d'anti-virus et la publication de correctifs ?

- x Protéger son infrastructure sur un périmètre vis-à-vis de l'extérieur avec un filtrage IP adéquat
- x Déployer de l'anti-virus pour cloisonner son réseau
- x Utiliser une mise à jour automatique des signatures
- x Gérer la sécurité des postes nomades
  - x Equiper chaque poste d'un système de sécurité complet
  - x Prévoir la gestion de mise à jour de l'anti-virus
  - x Faire un contrôle d'intégrité avant la connexion au réseau de votre organisme
  - x Préparer des procédures de sécurité et d'alerte en cas d'incident
    - x Information des utilisateurs par SMS
    - x Cellule de décontamination à l'entrée des batiments avec un CD-ROM

# Infogérance/télémaintenance : état des lieux

- x Le système d'information est interpénétré de part et d'autre par les infogérances et les télémaintenances
- x Relation contractuelle entre prestataire et client
- x Exemples en télémaintenance
  - x Routeurs chez les opérateurs de télécommunication
  - x PABX
  - x Imprimantes, télécopieurs, photocopieurs
  - x SAN : réseau de stockage de données
  - x Logiciels de gestion d'entreprise

# Infogérance/télemaintenance : perspectives

- x Appliquer sa politique de sécurité
- x Intégrer la sécurité dès le départ dans tout processus d'infogérance et de télémaintenance
  - x Contractuellement, systématiquement, ne serait-ce que pour savoir qu'il y a de la télémaintenance
- x Minimiser les télémaintenance
- x Créer un portail de contrôle d'accès
  - x Indépendamment des moyens de connexion
  - x Authentifier individuellement chaque télémainteneur
  - x Journaliser les connexions
  - x Recopier si possible la session complète des informations qui remontent à l'extérieur

- x Espace dont je suis responsable
  - x Le système d'information de l'entreprise
- x Espace dont je ne suis pas responsable
- x Je dois appliquer ma politique de sécurité entre les deux afin de protéger l'espace dont je suis responsable : **périmètre**
- x Il semble difficile de se passer de la notion de sécurité périmétrique même si le périmètre est poreux :
  - x Il faut donc savoir où est le périmètre
- x Quelques limites du périmètre :
  - x Le réseau et les canaux de communication
  - x Les utilisateurs
- x L'entreprise étendue

- x Le nouveau protocole de l'Internet dans les entreprises est HTTP/HTTPS
  - x Le nouveau protocole des entreprises sur Internet n'est pas IPv6
  - x La promotion des *Web Services* vise à ré-encapsuler tout un ensemble de protocoles sur HTTP au lieu de le faire sur IP, pour contourner le *firewall*
  - x Les logiciels d'EDI, de messagerie instantanée, d'agenda et de messagerie basés sur les *Web Services* sont très souvent des outils de contournement de la politique de sécurité de l'organisme
- x Les réseaux sans fil ouvrent une brèche dans l'aspect physique du périmètre du réseau
  - x Un réseau local sans fil se sécurise (sauf déni de service)
  - x Avec de la sécurité dans le réseau : 802.1X, indépendante des réseaux sans fil

- x Les télécommunications et l'Internet ne font qu'un
  - x Le PABX classique est un ordinateur Unix qui interroge l'annuaire d'entreprise
  - x Les téléphones utilisent des réseaux IP
  - x La télémaintenance par liaison téléphonique en PPP ne sert qu'à contourner le firewall sur les liaisons IP
  - x Les liaisons séries des immeubles intelligents passent aussi à IP
    - x RS232 devient Telnet sans authentification

- x Au début de l'informatique
  - x Un ordinateur pour beaucoup d'utilisateurs
- x Avec la micro-informatique
  - x Un micro-ordinateur par utilisateur
- x Actuellement
  - x Plusieurs ordinateurs par utilisateur
    - x Un micro-ordinateur au bureau
    - x Un micro-ordinateur chez soit
    - x Un ordinateur portable
    - x Un assistant personnel
    - x Un téléphone portable
    - x Etc
  - x Des ordinateurs achetés personnellement utilisés professionnellement

- x Si nécessaire se réorganiser
- x Production réseau/télécom vs sécurité
  - x La volonté de disponibilité du réseau est souvent difficilement compatible avec la politique de sécurité
  - x Il faut donc distinguer les équipes opérationnelles réseau et sécurité
  - x L'équipe réseau/telecom gère le réseau
  - x L'équipe sécurité gère les équipements sur le périmètre, dont la fonction principale est la sécurité
- x Production réseau/télécom vs téléphonie
  - x Le téléphone n'est plus un service général mais de l'informatique
  - x Il doit être géré par la production informatique

- × Accepter et gérer des moyens de connexions hétérogènes
  - × Le même PC portable ou assistant personnel est tantôt connecté au réseau d'entreprise :
    - Dans son bureau
    - Dans la salle de réunion
    - Via l'accès Internet ADSL de la maison
    - Via un modem GPRS dans le train
    - Via un HotSpot dans un aéroport
- × Accepter et gérer des plates-formes hétérogènes
  - × Intégrer dans le système d'information de l'entreprise les équipements choisis, achetés et appartenant à l'individu
  - × La monoculture est source de fragilité
  - × Fournir de quoi chiffrer pour tous les types d'assistants personnels
    - × PalmOS, Symbian, Windows CE, ...

- x Prévenir les systèmes de contournement du périmètre
  - x Exemples comparatifs
    - x Sprint PCS Business Connection : Ré-encapsulation de TCP/IP sur HTTP, serveur central chez Sprint
    - x Lotus Notes : Protocole propriétaire sur TCP/IP, serveur central dans l'entreprise
    - x Ipracom : Protocole propriétaire en UDP sur IP ré-encapsulé sur HTTP sur TCP/IP, pas de serveur central
    - x Enetshare : XMPP, XML et Webdav sur HTTP sur TCP/IP, serveur central dans l'entreprise
- x Intégrer les extensions de plages horaires

- x Reconcevoir les passerelles de sécurité sur le périmètre en prenant en compte :
  - x Analyse de contenu dans HTTP
    - x Recherche de protocoles re-encapsulés
    - x Anti-virus
  - x Protocoles de messagerie instantanées et de téléphonie
  - x Accès distants de toute nature
  - x Journalisation permettant des analyses statistiques

- x Cloisonner le réseau et intégrer la sécurité dans le réseau
  - x Le réseau est le dénominateur commun du système d'information
  - x Le réseau est le premier composant réellement sous le contrôle de l'entreprise
  - x Séparer les réseaux bureautique, supervision, téléphonie, etc
  - x Prévoir les commutateurs/firewalls et la prise en compte de l'espace hertzien
  - x Prévoir et accepter la sécurité entre les VLAN
  - x Authentifier équipements et utilisateurs
  - x Gérer dans le réseau des zones de confiance telles qu'elles existent dans l'entreprise

- x Applications développées dans l'entreprise principal maillon faible vis-à-vis de l'extérieur
- x Intégrer la sécurité dans le développement de ses applications
  - x Cahier des charges, formation, audit

- x Prendre en compte la sécurité et les conséquences de ce que l'on fait sur la sécurité
  - x Le fait de penser à la sécurité dans toutes les phases d'un projet, d'une décision, aide à l'amélioration de la sécurité
  - x La sécurité coute quand elle est prise à part
- x La sécurité est un facteur d'amélioration de la productivité et de la qualité
  - x La sécurité n'est pas un coût
  - x La sécurité apporte aussi un retour sur investissement
- x Un projet de sécurité est un projet comme un autre

## Questions ?

[Herve.Schauer@hsc.fr](mailto:Herve.Schauer@hsc.fr)

- x Sur [www.hsc.fr](http://www.hsc.fr) vous trouverez des présentations sur
  - x Infogérance en sécurité
  - x Sécurité des réseaux sans-fil
  - x Sécurité des SAN
  - x Sécurité des bases de données
  - x BS7799
  - x etc
- x A venir
  - x Retour sur investissement en sécurité