



HERVÉ SCHAUER CONSULTANTS

Cabinet de Consultants en Sécurité Informatique depuis 1989

Spécialisé sur Unix, Windows, TCP/IP et Internet

Convergence sécurité logique et sécurité physique ?



Development Institute International

**Forum 2005 de la Sécurité Bancaire
8 décembre 2004**

Hervé Schauer

<Herve.Schauer@hsc.fr>

- x HSC
- x Quelques exemples de problèmes et d'enjeux en sécurité
 - x Vers et virus
 - x Infrastructures
 - x Pourriel (SPAM) et hameçonnage (*phishing*)
 - x Infogérance/Télémaintenance
- x Où est le périmètre de l'entreprise ?
 - x Implication du nomadisme et de la voix sur IP
- x Sécurité physique et logique : quelles imbrications ?
- 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 Conseil, études, audits, tests d'intrusion, formations
- x Domaines d'expertise
 - x Sécurité Windows/Unix/systèmes embarqués
 - x Sécurité des applications
 - x Sécurité des réseaux : TCP/IP, PABX, réseaux opérateurs, avionique, ...
 - x Organisation de la sécurité
- x Clients : ① Opérateurs telecom, ② Banques , ③ Etat
- x Certifications
 - x CISSP, BS7799 Lead Auditor, ProCSSI

- x Virus et vers
 - x Constat
 - x Exemple de Blaster (août 2003)
 - x Etat des lieux / Perspectives
- x Infrastructures
 - x Exemple du déni de service Cisco (juillet 2003)
 - x Exemple des pannes opérateurs (octobre/novembre 2004)
 - x Perspectives
- x Pourriel (SPAM) et hameçonnage (*phishing*)
 - x Etat des lieux et perspectives
- x Infogérance/Télemaintenance
 - x Etat des lieux / Perspectives

- x Dénis de services et chantages aux dénis de service
- x Gestion des correctifs de sécurité et des mises à jour
- x Maîtrise des réseaux sans fil
- x Contrôle des postes de travail
- x Migration vers des solutions d'identification/authentification universelles
- x Journalisation et tableaux de bords en sécurité
- x Téléphonie sur IP
- x Intégration des ordinateurs nomades et assistants personnels

- 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 Se réplique par des ports de communication normalement fermés par les *firewalls*
- x Est volontairement très lent, environ 2000 ordinateurs par heure
- x Ciblait à terme un déni de service que un serveur : 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 S'est dupliqué sur des réseaux non connectés 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 Mettre en quarantaine les systèmes compromis
 - x Préparer des procédures de sécurité et d'alerte en cas d'attaque de vers
 - x Information des utilisateurs par SMS
 - x Cellule de décontamination à l'entrée des bâtiments avec un CD-ROM

- x Socle sur lequel tout repose
- x Ensemble de matériels et logiciels auquel il faut faire confiance
 - x Ordinateurs, routeurs, applications
- x Fragilité des routeurs : exemple du déni de service sur les routeurs Cisco
- x Exemple des pannes des opérateurs
- x Perspectives

Exemple du déni de service Cisco (1/3)

- x L'internet et les réseaux s'entreprennent reposent sur des routeurs Cisco
- x Déni de service sur tous les équipements Cisco publié le 17 juillet 2003
 - x Envoi de paquets dirigés vers le routeur sur certains protocoles précises de manière à ce que le paquet s'arrête sur le routeur
 - x Les paquets mis dans la file d'attente n'est alors jamais traité par le routeur
 - x La file d'attente se remplit après 75 paquets par défaut.
 - x Le routeur n'est plus accessible et ne traite plus les paquets entrants sur cette interface.
- x Concerne tous les équipements du plus petit au plus important
 - x Les routeurs personnels comme les commutateurs ou les équipements au coeur des infrastructures des opérateurs

- x **Exploitation triviale**

- x Commande **hping** sur Unix en usurpant l'adresse source ou en changeant d'adresse à chaque paquet
- x Cisco a publié une version corrigée de son système pour chaque plateforme et chaque branche
- x Les opérateurs de premier niveau ont été prévenus en avance :
 - x Ils ont pu mettre à jour rapidement leurs équipements
 - x Il y a eu plus de perturbations liées aux mises à jour que pour des attaques
- x Certains opérateurs ont mis des filtres
 - x Sur les équipements le supportant, sur les routeurs peu chargés, ou sur les routeurs d'extrémité, mais beaucoup les ont supprimés depuis

- x Les routeurs des réseaux d'entreprises n'ont généralement pas été mis à jour suite à la publication du problème
- x Ver style Slammer ou Blaster
 - x Il reste des vulnérabilités non exploitées dans Windows
 - x Insertion d'un portable contaminé dans le réseau
- x Recherche des routeurs locaux
- x Attaques simultanées des routeurs en commençant par les routeurs les plus éloignés découverts
- x L'ensemble des réseaux d'entreprises sont inopérants
 - x Relance manuelle de chaque boitier par un administrateur système
 - x Quelques minutes / heures mais quelles cascades ?

- x Passerelle de conversion de téléphonie sur IP en téléphonie classique
 - x Transformation par la passerelle de numéros de téléphones usurpés en téléphonie sur IP en numéros internationaux illégaux
 - x Déclenchement d'alarmes sur les centraux téléphoniques et refus de prise en charge d'appels légitimes
 - x Erreur de conception dans le logiciel de la passerelle : les appels auraient du être refusés par celle-ci
- x Equipement d'aiguillage des communications
 - x Blocage après la mise à jour de l'application du boîtier
 - x Basculement sur le système en redondance et blocage identique
 - x Erreur dans l'application identique sur les deux systèmes
- x Pannes applicatives

- x Envisager et se préparer aux scénarios d'attaques et de panne
- x Imposer l'évaluation de la sécurité de ses équipements d'infrastructure
 - x A défaut faire auditer leur sécurité par un tiers
- x Privilégier la diversité dans les équipements réseau
 - x Utiliser des équipement de secours de marque différente que l'équipement de production
 - x Prévoir un plan de reprise sur la version précédente du logiciel de l'équipement
 - x Imposer une interopérabilité pour bénéficier d'équipements en redondance de fournisseurs différents
- x Ne pas accepter de dépendance auprès d'un seul fournisseur
- x Ne pas accepter l'inapplicabilité de sa politique de sécurité sur ses équipements

- x Constat sans doute inutile
- x Critères de choix de solutions
 - x Taux de faux-positifs < 0,01%
 - x Taux d'efficacité dans le filtrage
 - x Facilité de gestion des messages bloqués
 - x Facilité d'intégration des spécificités des messages échangés par son organisme
 - x Penser à l'infogérance du service
- x Perspectives
 - x Modèles fermés ?
 - x Facturation à l'émetteur ?
 - x ...

- x Vol du compte de service de banque en ligne
 - x Objectif classique : détournement de fonds par un virement
 - x Envoi d'un message faisant croire à la victime qu'elle doit se connecter sur un site de la banque
 - x Le site n'est pas celui de la banque mais celui du pirate
 - x Le pirate récupère les informations d'identification et d'authentification
 - x Il se connecte à la banque à la place de la victime
- x La banque cible de l'attaque n'est pas directement attaquée
 - x C'est le client de la banque qui est attaqué
- x Au moins 3 cas en 2004 en France

- x Sensibilisation des utilisateurs des services de banque en ligne
- x Contrôle de la déclaration des comptes destinataires de virements
 - x Imposer la connaissance d'un nombre non-devinable qui est sur le relevé papier
- x Journalisation fonctionnelle dans les applications
- x Détection des anomalies et analyse humaine
 - x Connexion sur plusieurs comptes depuis la même plage d'adresse, virement complet vers un compte externe, ...
 - x Mise en attente des transactions suspectes et appel téléphonique du chargé de clientèle à l'usager
- x Aucune raison de réduire l'étendue et la qualité du service auprès des usagers
 - x Suppression des possibilités de virement, réduction drastique des montants autorisés
 - x Authentification forte, carte à puce, refus des utilisateurs de Mac et de Linux

Infogérance/télémaintenance : état des lieux

- x Le système d'information est inter-pénétré 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 des 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 logique 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 : toutes les applications dialoguant avec l'extérieur

- 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 de nombreux 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 soi
 - 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

- × Reconcevoir les passerelles de sécurité sur le périmètre en prenant en compte :
 - × Analyse de contenu dans HTTP
 - × Recherche de protocoles re-encapsulés
 - × Anti-virus
 - × Protocoles de messagerie instantanées et de téléphonie
 - × Accès distants de toute nature
 - × 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 confiances telles qu'elles existent dans l'entreprise

- x Applications développées dans l'entreprise principal maillon faible vis-à-vis de l'extérieur
- x Tout application visible de l'extérieur est sur le périmètre
- x Intégrer la sécurité dans le développement de ses applications
 - x Cahier des charges, formation, audit
 - x Journalisation fonctionnelle
 - x Analyse des entrées et des sorties
 - x Lutte contre les injections de code (SQL, LDAP, etc)
 - x Lutte contre l'exécution croisée de code (*Cross-Site-Scripting*)
- x Prévoir des systèmes de sécurité applicatif

- x Le périmètre logique doit rejoindre le périmètre physique
- x Les défaillances des équipements doivent plus être envisagées comme des pannes matérielles mais aussi logicielles
- x Contrôle d'accès physique par des moyens logiques
 - x Badgeuses
 - x Videosurveillance sur IP
- x Immeubles intelligents
 - x Migration de liens série vers des communications Telnet sur IP
 - x Supervision avec des serveurs Windows
 - x Mise à jour de l'anti-virus ? Des correctifs de sécurité ?
 - x Infogérance du système depuis le site de la société de gardiennage
 - x Interconnexion sur internet ?

- 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 coûte quand elle est prise à part
- x Exploiter les exemples d'incidents pour sensibiliser et améliorer ses scénarios de risques
- x Refaire son analyse de risque en intégrant les perspectives technologiques

Questions ?

Herve.Schauer@hsc.fr

- x Sur **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 SPAM
 - x BS7799
 - x etc

- x Sur **www.hsc-news.com** vous pourrez vous abonner à la **newsletter HSC**