



HERVÉ SCHAUER CONSULTANTS

Cabinet de Consultants en Sécurité Informatique depuis 1989

Spécialisé sur Unix, Windows, TCP/IP et Internet

# La sécurité & la direction informatique



**DSI 2004**

**6 octobre 2004**

**Hervé Schauer**

<Herve.Schauer@hsc.fr>

- x HSC
- x Contexte DSI & enjeux en sécurité
- x Progiciel
- x Vers et virus
- x SPAM
- x Infogérance/Télemaintenance
- x Périmètre
- x Applications
- x ROSI
  - x Coûts de la sécurité, courants d'approche du ROSI, choix
- 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, audits, 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 Organisation de la sécurité
- x Certifications
  - x CISSP, BS7799 Lead Auditor

- 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 Maîtrise 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 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](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 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 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

- 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 ...

# 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 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 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

- 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 ROSI : *Return On Security Investment*
- x ROSI vient de ROI : *Return On Investment*
- x Gain financier d'un projet de sécurité au regard de son coût total
  - x Net : en monnaie constante
  - x Investissements et fonctionnement
  - x Sur une période d'analyse donnée
- x TCO : coût total associé au cycle déploiement/maintenance
- x Le ROSI relativise les coûts par rapport aux bénéfices
  - x Point de retour : Date à partir de laquelle les gains dépassent les coûts
- x Le ROSI est plutôt la valeur ajoutée d'un investissement en sécurité
  - x Plus de notion financière uniquement

- x La manière de travailler repose sur des chiffres de coûts
  - x Les dirigeants prennent leurs décisions face à des tableaux Excel
- x Dans nos présentations de résultats d'audit, une demande récente est d'établir des tableaux de coûts associés aux risques encourus et aux recommandations proposées
- x Les raisons historiques du pourquoi fait-on de la sécurité ne leur suffisent plus
  - x Principaux facteurs d'influence actuels auprès des directions :
    - x Sensibilisation à la gestion des risques
    - x Contraintes réglementaires

- × Coûts organisationels, humains, techniques
  - × La sécurité est de l'organisation et des hommes
  - × La sécurité n'est pas des licences logicielles
- × **Coûts ponctuels**
  - × Mise en place des dispositifs de sécurité
  - × Conséquences directes des incidents de sécurité
- × **Coût récurrents**
  - × Exploitation et contrôle
  - × Plus des 2/3 du coût total
- × **Coûts tangibles**, mesurables
  - × Perte de productivité, de revenus
  - × Coûts de reconstitution, d'assurance
- × **Coût intangibles**, difficilement mesurables
  - × Perte de réputation, de part de marché
  - × Poursuites juridiques

- x Divers arguments évoqués dans la littérature
- x Arguments technologiques
  - x Généralisation d'outils ou de procédures
  - x Réduction du nombre d'incidents
  - x Amélioration de la convivialité pour les utilisateurs
- x Arguments métiers
  - x Analyse de risque, assurance, concurrence dans le secteur
- x Arguments réglementaires et normatifs
  - x Lois : Sarbanes-Oxley, sécurité financière, informatique & libertés
  - x Normes : BS7799
  - x Liés au métier : CRBF 97-02, Bâle II, HIPAA

- x Issus des travaux du Clusif ([www.clusif.asso.fr](http://www.clusif.asso.fr))
- x Amélioration de la productivité
  - x Pas spécifique à la sécurité
- x Diminution des incidents
- x Analyse de risque
- x Enjeux métiers
- x Meilleures pratiques
- x Benchmarking

- x ALE : Annual Loss of Expectancy

- x Pertes annuelles prévisibles à partir de la fréquence de survenance d'un incident et coût financier de son impact
- x ROSI : différence entre l'ALE actuel et l'ALE futur + le coût de la solution

- x Limites

- x Calcul de probabilité donc bases d'incidents et effort de modélisation
- x Pas de distinction entre occurrence faible/impact élevé et occurrence élevée/impact faible

- x Exemple

- x Scénario

- x Attaque virale généralisée coûterait 1M€ avec une probabilité d'occurrence de 70%

- x Solution

- x Diminution de la probabilité de 20% par le déploiement d'une nouvelle infrastructure anti-virale de 150 k€

- x ROSI

- x  $70\% \times 1\text{M€} - (70-20)\% \times 1\text{M€} - 150 \text{ k€} = 50 \text{ k€}$

- x Comparaison du **risque potentiel maximal** par rapport au coût de la solution
- x Avantage : approche largement employée
- x Limites
  - x Technique de quantification différentes d'une méthode à une autre, d'un expert à l'autre
  - x Scénarios de risques non-exhaustifs et hypothèses des scénarios susceptibles d'être remises en cause
- x Exemple
  - x Scénario
    - x Serveur de production sur un site non-sécurisé redondé localement, en cas de sinistre majeur sur le site la perte est évaluée à 15M€
  - x Solution
    - x Hébergement sur un site distant sécurisé : 4M€
  - x ROSI
    - x Coût de la solution de 4M€ par rapport à celui du sinistre de 15M€

- x La sécurité est génératrice de richesses dans votre activité
  - x Gain de part de marché, avantage concurrentiel
  - x Amélioration de la qualité d'un service, de l'image de marque
- x Avantage : utilise le langage métier et fédère l'organisme
- x Limites
  - x N'utilise pas d'analyse coût/bénéfices
  - x Difficile à expliquer et d'atteindre les bons interlocuteurs
- x Exemple
  - x Scénario
    - x Serveur d'assurance avec fichier nominatif non-protégé : clients, biens assurés, ...
  - x Solution
    - x Sécurisation du serveur, ajout d'un contrôle d'accès, authentification forte
  - x ROSI
    - x Enjeu lié à l'image et au risque juridique

- x **Avantage**

- x Approche de plus en plus acceptée
- x Alternative à l'analyse de risque

- x **Limite**

- x Beaucoup pensent que les meilleures pratiques ne sont pas pour eux

- x **Exemple**

- x **Scénario**

- x Un audit de sécurité révèle que l'ERP d'une société cotée n'a pas de ségrégation des tâches et de traçabilité, ouvrant la possibilité à des fraudes internes

- x **Solution**

- x Intervention d'un cabinet d'expertise en sécurité pour reconstruire la sécurité applicative

- x **ROSI**

- x La direction n'étant pas sensibilisée à la fraude interne c'est le respect de la loi sur la sécurité financière qui les a fait décider

- x Comparatif de performance des entreprises
- x Avantages
  - x Les dirigeants apprécient
- x Limites
  - x Ne prend pas en compte les spécificités locales et pousse à agir de façon identique
- x Exemple
  - x Scénario
    - x Un audit de sécurité de service en ligne révèle un serveur très mal conçu où tous les clients peuvent visualiser les informations des tiers. Jamais un service du secteur n'a été vu dans un tel état.
  - x Solution
    - x Ré-écrire l'application
  - x ROSI
    - x Rejoindre la majorité, ne pas faire pire que les autres

- x Combiner toutes les approches de ROSI fonctionnant pour son projet
  - x Risques
  - x Sinistralité
  - x Enjeux business
  - x Amélioration de la productivité
- x Utiliser la cartographie d'orientation suivant le :
  - x Type de projet :
    - x Projet plutôt métier, financé par une maîtrise d'ouvrage opérationnelle ou fonctionnelle
    - x Projet plutôt sécurité
  - x Contexte économique, humain et intrinsèque aux projets
- x Permet de combiner aspects quantitatif et qualitatif

- x Gérer la sécurité comme un projet comme les autres
- x Réunir les arguments
  - x Objectifs stratégiques
  - x Economies d'échelle
  - x Contraintes réglementaires
  - x Alignement avec la culture d'entreprise
  - x Plan de financement
- x Solliciter les acteurs-clés
  - x Contrôle interne, finance, management

- 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 Considérer les projets de sécurité comme les autres
  - x La sécurité est un facteur d'amélioration de la productivité et de la qualité
  - x Le ROSI est un instrument sophistiqué mais la sécurité n'est pas juste un coût
  - x La sécurité apporte aussi un retour sur investissement

## Questions ?

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