

MSSP ou fournisseurs de services d'infogérance en sécurité

Conférence CLUSIF
24 juin 2002

Hervé Schauer
<Hervé.schauer@hsc.fr>

Hervé Schauer Consultants
<<http://www.hsc.fr/>>



Copyright Hervé Schauer Consultants 2002 – Reproduction interdite

Fournisseurs d'infogérance en sécurité. Agenda (1/2)

- Hervé Schauer Consultants
- Définition du MSSP
- Intérêt de l'entreprise pour un MSSP
- Le besoin des MSSP
- La hiérarchie et le RSSI
- Infogérance
- Marché de l'infogérance en sécurité par le MSSP
- Les types de MSSP

Copyright Hervé Schauer Consultants 2002 – Reproduction interdite – www.hsc.fr



Fournisseurs d'infogérance en sécurité. Agenda (2/2)

- Méthodologie
 1. Décision de faire de la sécurité
 2. Décision de faire appel à l'infogérance
 3. Fabrication d'un appel d'offre
 4. Analyse des propositions
 5. Accord sur les contrats de service
 6. Consensus sur les procédures de travail
 7. Implémentation
 8. Gestion de la relation dans le temps
- Cas des ASP de test de vulnérabilités
- Résumé
- Conclusion
- Références et Ressources

Copyright Hervé Schauer Consultants 2002 – Reproduction interdite – www.hsc.fr



Hervé Schauer Consultants (1/2)

- Cabinet de consultants en sécurité Unix, Windows, TCP/IP et Internet depuis 1989
- 14 consultants

- Expérience de la sécurité Unix depuis 1987
- Expérience de la sécurité Internet depuis 1991
- Expérience de la sécurité Windows depuis 1997

- Conception et architecture
 - Sécurité Internet/Intranet
 - Détection d'intrusion
 - Commerce électronique et services en ligne

- Mise en place de systèmes de sécurité

Copyright Hervé Schauer Consultants 2002 – Reproduction interdite – www.hsc.fr



Hervé Schauer Consultants (2/2)

- Audits de sécurité techniques et par rapport à un référentiel
 - Réseaux, réseaux sans-fil, applications, code, etc
- Enquêtes après intrusion
- Tests d'intrusion et de vulnérabilités

- Veille en vulnérabilités
- Veille technologique de l'actualité en sécurité

- Programme complet de 12 formations en sécurité

- Plus de 30 produits de sécurité maîtrisés
- Plus de 200 références dans tous les secteurs d'activités et sur tous les continents
- Basé à Paris, avec une agence à Toulouse

Copyright Hervé Schauer Consultants 2002 – Reproduction interdite – www.hsc.fr



Définition du MSSP (1)

- Qu'est-ce que les fournisseurs d'infogérance de services en sécurité ou *Managed Security Services Providers : MSSP* ?

- Une gestion et une surveillance de périphériques ou systèmes dont la fonction principale est la sécurité
 - Infogérance de firewalls
 - Centralisation et traitement des journaux
 - Infogérance de logiciels de détection d'intrusion
 - Tests de vulnérabilités
 - Infogérance de VPN chiffrés
 - Infogérance d'anti-virus
 - Services d'authentification des utilisateurs
 - Hébergement d'infrastructure de clés

Copyright Hervé Schauer Consultants 2002 – Reproduction interdite – www.hsc.fr



Définition du MSSP (2)

- Pourraient aussi être considérés d'autres services
 - Infogérance d'hébergement sécurisé
 - Serveurs web
 - Plates-formes de commerce électronique

 - Infogérance de services de sécurité de secours

Intérêt pour une entreprise d'avoir un MSSP

- Les gains de l'utilisation d'un MSSP vu par l'entreprise
 - Permettre de réduire les coûts
 - Fournir un service 24h/24h
 - Éviter d'avoir ses propres centres d'exploitation des équipements de sécurité
 - Maintenir ou améliorer la sécurité existante

Les besoins de MSSP

- Les systèmes devant être vus comme gérants principalement de la sécurité se sont multipliés
 - Manque de personnel
 - Difficulté à suivre tous les projets
 - Difficulté à se focaliser sur ce qui est important
 - Manque de temps pour former les gens
 - Organisation et industrialisation difficiles
 - Pas le bon administrateur qui a la bonne information
 - Pas d'application rapide et globale des correctifs de sécurité
 - Plans de continuité difficiles à faire

Direction et RSSI

- Direction
 - Le RSSI s'occupe de la sécurité, c'est délégué donc c'est réglé
 - Pas ou très peu de conscience de leurs responsabilités vis-à-vis de la sécurité
 - Manque de responsabilités légales ?
 - Le RSSI veut plus de personnel : qu'il achète ailleurs au lieu de construire son service à lui
 - Sécurité pas le coeur du métier
 - Pourquoi ne sait on pas gérer Code Red ou Nimda ?
 - Il ne vous plaît pas mon accès sans fil ?
 - Il faut faire du 24h/24h
- Le RSSI
 - Infogérer la sécurité est un non-sens
 - Infogérer la sécurité va augmenter ma charge de travail

Infogérance

- L'infogérance s'apprend
- L'infogérance n'est pas facile
- L'infogérance demande de l'expérience
- La sécurité est plutôt ce qu'il faut infogérer en dernier
- Il ne faut sans doute pas infogérer de la sécurité sans expérience préalable significative dans l'infogérance

Marché de l'infogérance de la sécurité

- La France n'est pas le marché le plus mature, mais en forte croissance
- L'infogérance est moins dans la culture ou l'état d'esprit que dans les pays anglo-saxons
- MSSP et ASP en sécurité souvent apparus avec la vague des startups Internet
 - Concentration des investissements du capital risque en sécurité depuis 2 ans dans ces entreprises
- Les noms cités sont illustratifs et ne sont pas exhaustifs
 - Désolé pour ceux qui ne me sont pas venus à l'esprit

Les types de MSSP (1/4)

- Sociétés de conseil
 - Big 5 : Accenture, D&T, E&Y, KPMG, PWC
 - Souvent avec des partenariats
 - HSC

- Intégrateurs
 - Parfois avec des partenariats
 - Alcatel
 - Integralis / Allasso / Activis
 - Telindus-CF6
 - Thales
 - Ubizen / Risc Technology
 - Via Networks
 - Transiciel

Les types de MSSP (2/4)

- SSII
 - ATOS
 - Bull Integris
 - Cap Gemini
 - EDS
 - Steria

- Startups
 - Counterpane
 - Intexxia
 - Intranode
 - Neoteris
 - Netcelo
 - Openreach
 - Smartpipes
 - Qualys

Les types de MSSP (3/4)

- Éditeurs de logiciels de sécurité
 - Infogèrent principalement leurs logiciels
 - ISS
 - NAI
 - Symantec
 - Trendmicro

- Vendeurs de plates-formes
 - Compaq / HP
 - IBM
 - Nortel
 - Sun
 - Avec des partenariats pour certains services

Les types de MSSP (4/4)

- ISP / Telcos
 - BT
 - Cable & Wireless (ISDnet)
 - Cegetel
 - Colt
 - Equant / France Telecom / Olean
 - UUnet
 - Avec parfois des partenariats

Méthode : phases

- 1) Décision de faire de la sécurité
- 2) Décision de faire appel à l'infogérance

- 3) Fabrication d'un appel d'offre
- 4) Analyse des propositions
- 5) Accord sur les contrats de service
- 6) Consensus sur les procédures de travail

- 7) Implémentation
- 8) Gestion de la relation dans le temps

Décision de faire de la sécurité

- L'infogérance ne résout pas la sécurité en elle-même

- Il faut avoir une politique de sécurité déjà déployée

- Conscience de la sécurité par les responsables de l'entreprise
 - PDG, Directeur informatique, Directeur financier, etc

- Quel est mon métier ?
- Qu'est-ce qui fait la valeur de mon entreprise ?
- Qu'est-ce que je souhaite protéger ?
- Est-ce que mon système d'information est partie intégrante de ma compétitivité ?

Décision de faire appel à l'infogérance

- Définir les objectifs en terme de métier
- Définir les objectifs en terme de résultat attendu
 - Indépendamment de la technologie
- Lister les technologies utilisées ou souhaitées pour répondre aux résultats attendus
- Choisir lesquelles seront mises en infogérance en premier
 - Ce que l'on ne sait pas faire et qui a facile à sous-traiter
 - tests de vulnérabilités sur son périmètre
 - Ce qui est répétitif et industrialisé
 - Firewalls, VPN IPsec
 - Ce que l'on saura surveiller sans le gérer
- Au besoin faire un audit de l'existant ou une analyse de risques
- Lister les freins au succès de l'opération par rapport à une gestion en interne
- Documenter le tout par écrit avant de passer à la phase suivante

Copyright Hervé Schauer Consultants 2002 – Reproduction interdite – www.hsc.fr



Fabrication d'un appel d'offres

- Définir le service souhaité
 - Fonction
 - Disponibilité
 - Échelle
 - Surveillance et rapports
 - Performance
 - Gestion
 - Suivi
- Définir la sécurité et décrire les techniques souhaitées
- Définir les moyens
 - Humains
 - Secours

Copyright Hervé Schauer Consultants 2002 – Reproduction interdite – www.hsc.fr



Analyse des propositions (1/2)

- Expérience de l'infogéreur
- Références dans le domaine
- Répond à l'ensemble des besoins actuels et à venir
- Dépendance à d'autres fournisseurs via des partenariats

- Méthodes de travail
- Technologies utilisées

- Existence d'audits par des tiers
 - Techniques du centre opérationnel
 - Infrastructure, configuration des serveurs
 - Applications, code
 - Organisationnels et méthodologiques : procédures, personnel
 - Pertinence et compétence des tiers auditeurs
 - Disponibilité des rapports d'audit

Copyright Hervé Schauer Consultants 2002 – Reproduction interdite – www.hsc.fr



Analyse des propositions (2/2)

- Capacité d'une approche personnalisée
 - Permettre les adaptations spécifiques

- Système de suivi et de surveillance performant
 - Voir si une règle de sécurité a été changée
 - Voir si un VPN est tombé
 - Recevoir les alarmes
 - Bénéficier d'un service d'analyse en cas d'incident

- Partage de responsabilité en cas d'incident

Copyright Hervé Schauer Consultants 2002 – Reproduction interdite – www.hsc.fr



Accord sur les contrats de service

- Synthèse de l'appel d'offre et de la proposition
 - Précision, exhaustivité, détails
- Service rendu
- Rôles et responsabilité des parties
- Renouvellement, terminaison et transfert du contrat
- Accès du client
 - Journaux : accès, conservation, analyse
- Audit par un tiers
- Assurance

Consensus sur les procédures de travail

- Documentation et procédures de l'infogéreur
 - Accès physique
- Documentation de ce qui n'est pas contractuel
 - Dialogues
 - Accès
 - Création et suppression des comptes
 - Contrôle
 - Procédures en cas d'incident
 - Responsabilités

Implémentation

- Projet similaire à beaucoup d'autres projets

Gestion de la relation dans le temps

- Réunions de suivi et gestion des évolutions
 - Évolutions technologiques
 - Mise à jour des procédures de travail
- Audits par des tiers
 - Revue de résultats
 - Mise en place de mesures
- Réunion de bilan
 - Mise à jour contractuelles

Le cas des ASP de tests de vulnérabilité (1/2)

- Service populaire mais limité
- Scanner un réseau à distance n'est pas une science exacte
 - Il faut de l'expérience pour valider les résultats
 - Un scanner peut rater un port FTP ouvert et vulnérable à une chaîne de format car le réseau est chargé,
 - La vulnérabilité est majeure
 - Le résultat du test est faux
- Scanner les ports d'un serveur est simple
 - Comment vérifier depuis une station d'administration si un port TCP est ouvert sur un serveur linux ?

- `ssh srvX netstat -anlA inet > ports-srvX ; diff ports-srvX ports-srvX.1`

Copyright Hervé Schauer Consultants 2002 – Reproduction interdite – www.hsc.fr



Le cas des ASP de tests de vulnérabilité (2/2)

- Donner des détails inutiles n'est pas un plus
 - Si un port 25/tcp est ouvert sur un serveur Web, il doit être fermé et filtré, inutile de connaître la version du logiciel derrière pour mettre en oeuvre la correction
- Prendre en compte les plates-formes de commerce électronique avec seulement HTTPS (443/tcp) et authentification des clients n'est pas facilement automatisable
 - Les vulnérabilités potentielles ne sont pas recherchées
 - `cgi-bin/valide_commande?commande=xterm%20-display%20x.x.x.x:0.0|`
- Prendre en compte les applications devient indispensable
- Service peu coûteux

Copyright Hervé Schauer Consultants 2002 – Reproduction interdite – www.hsc.fr



Résumé

- Comment allez vous gérer les journaux ? Faire des corrélations et les analyser ? Ou simplement les reformatter et me les renvoyer ?
- Comment supervisez vous les périphériques de mon entreprise ?
- En quoi votre service impacte mes équipes ?
- Fournissez vous à mes équipes un accès permanent à des données significatives et temps-réel ?
- Quand vous identifiez une attaque, quelles actions faites vous ?
- Quelle aide proposez vous pour associer ma politique de sécurité et votre service ?

Copyright Hervé Schauer Consultants 2002 – Reproduction interdite – www.hsc.fr



Conclusion

- Politique de sécurité et direction sensibilisée avant l'infogérance
- Infogérance en sécurité demande de l'expérience et de la méthode
- Bien sélectionner les services à infogérer
- Ne pas choisir sur le prix
- Toujours analyser le fond et le retour global sur investissement

Copyright Hervé Schauer Consultants 2002 – Reproduction interdite – www.hsc.fr



Références

- Fournisseurs de Services en Sécurité, Comment les utiliser ?
 - Hervé Schauer, HSC, Eurosec 2002, Paris, 02/02
 - www.hsc.fr/ressources/presentations/eurosec02/
- Technology Risk Managment for Outsourced Relationship
 - Faith Boetger, BITS, RSA Conference, San Jose, 02/02
- Six questions à poser à votre MSSP
 - Riptech, 02
 - www.riptechnology.com/sixquestions/intro.html

Copyright Hervé Schauer Consultants 2002 – Reproduction interdite – www.hsc.fr



Ressources

- Comment choisir son fournisseur de services d'infogérance en sécurité?
 - Hervé Schauer, HSC, Le Guide de la Sécurité des Systèmes d'Information et Internet, 02/02
 - www.hsc.fr/ressources/articles/infogérance/
- Managing Technology Risk for IT - Service Provider Relationships
 - BITS working group from the Financial Services Roundtable
 - www.bitsinfo.org/FrameworkVer32.doc

Copyright Hervé Schauer Consultants 2002 – Reproduction interdite – www.hsc.fr

