



Infogérance / Télémaintenance et sécurité

Forum Gartner - EXP/BLG
11 mai 2005

Gartner

Hervé Schauer
<Herve.Schauer@hsc.fr>

- Société de conseil en sécurité informatique depuis 1989
- Prestations intellectuelles d'expertise en toute indépendance
 - Pas de distribution, ni intégration, ni infogérance, ni investisseurs, ni délégation de personnel
- Prestations : conseil, études, audits, tests d'intrusion, formations
- Domaines d'expertise
 - Sécurité Windows / Unix et linux / embarqué
 - Sécurité des applications
 - Sécurité des réseaux
 - TCP/IP, téléphonie, réseaux opérateurs, réseaux avionique, ...
 - Organisation de la sécurité
- Certifications
 - CISSP, BS7799 Lead Auditor, ProCSSI

- Première partie reprise de ma présentation de mars 2002 à Eurosec
- Seconde partie réalisée récemment

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

- Infogérances : définitions
- Intérêt des entreprises pour les MSSP
- Le besoin des MSSP
- La hiérarchie et le RSSI
- Infogérance
- Marché de l'infogérance en sécurité par le MSSP
- Les types de MSSP

- Méthodologie
- 1) Décision de faire de la sécurité
- 2) Décision de faire appel à l'infogérance
- 3) Fabrication d'un appel d'offres
- 4) Analyse des propositions
- 5) Accord sur les contrats de service
- 6) Consensus sur les procédures de travail
- 7) Mise en oeuvre
- 8) Gestion de la relation dans le temps

- Questions à poser
- Télémaintenances
- Contournement par HTTP/HTTPS
- Télémaintenance : recommandations
- Ecueils
 - Exemple avec l'infogérance des accès distants au SI
- Conclusion
- Prochains rendez-vous
- Références et Ressources

- 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

- Pourraient aussi être considérés d'autres services
 - Infogérance d'hébergement sécurisé
 - Hébergement de serveurs web
 - Hébergement de plates-formes de commerce électronique
 - Hébergement de services administratifs en ligne
 - Services de diffusion distribuée
- Infogérance de services de sécurité de secours

- 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 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 et consommateurs de ressources

- Direction
 - Le RSSI s'occupe de la sécurité, c'est délégué donc c'est réglé
 - Parfois manque 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

- 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

- La France n'est pas le marché le plus mature, mais en 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
- Beaucoup d'investissements du capital risque en sécurité dans l'infogérance
 - Alors que c'est une activité de service à marge faible
- Les noms cités sont illustratifs et ne sont pas exhaustifs
 - HSC connaît les infogéreurs en étant auditeur en sécurité pour le compte de leurs clients

- Sociétés de conseil
 - "Big 5" : Accenture, D&T, E&Y, PWC
 - Souvent avec des partenariats et parfois via des filiales
 - De nombreuses sociétés se présentant comme sociétés de conseil en sécurité font leur chiffre d'affaires et leurs marges sur d'autres services dont l'infogérance
- Intégrateurs
 - Sont très nombreux, parfois avec des partenariats et en infogérant eux-mêmes le service à des tiers
 - Cybertrust (Betruusted / Ubizen)
 - Integralis / Allasso / Activis
 - NextiraOne, Telindus, Thales, etc

- SSII
 - ATOS, Devoteam, Bull Integris, Cap Gemini / Transiciel, EDS, Osiatis, Steria, ...
- *Startups*
 - Dont certaines ont disparues
 - Counterpane
 - Intexxia, Intranode, Qualys
 - Neoteris, Netcelo, Openreach, Ornis, Smartpipes

- Éditeurs de logiciels de sécurité
 - Infogèrent principalement leurs logiciels mais ont parfois des offres très larges
 - ISS, McAfee, Symantec, Trendmicro
- Vendeurs de plates-formes
 - HP
 - IBM
 - Nortel
 - Sun
 - Avec des partenariats pour certains services

- Opérateurs / ISP
 - 9telecom, BT, Cable & Wireless, Cegetel, Colt
 - France Telecom
 - Transpac, Oleanne, Equant, Orange, Wanadoo, FTH, ...
- Hébergeurs
 - Amen / Vianetworks
 - CVF
 - Prosodie

- 1) Décision de faire de la sécurité
- 2) Décision de faire appel à l'infogérance
- 3) Fabrication d'un appel d'offres
- 4) Analyse des propositions
- 5) Accord sur les contrats de service
- 6) Consensus sur les procédures de travail
- 7) Mise en oeuvre
- 8) Gestion de la relation dans le temps

1) Décision de faire de la sécurité

- L'infogérance ne résout pas la sécurité en elle-même
 - La décision primaire est de mettre en oeuvre un firewall
 - Pas d'acheter un service d'infogérance de firewall
- 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 ?

2) 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 est 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

2) Décision de faire appel à l'infogérance

- 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

3) 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

4) Analyse des propositions

- 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

4) Analyse des propositions

- 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

4) Analyse des propositions

- 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

5) Accord sur les contrats de service

- Synthèse de l'appel d'offres 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

6) 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

7) Mise en oeuvre

- Projet similaire à beaucoup d'autres projets

8) Gestion de la relation dans le temps

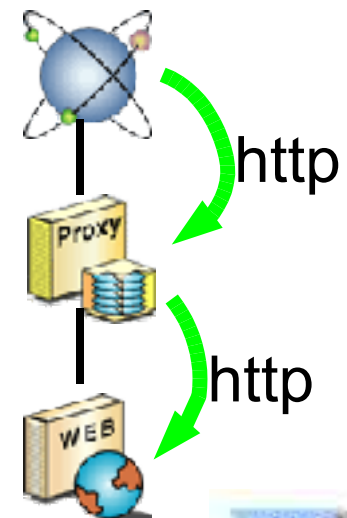
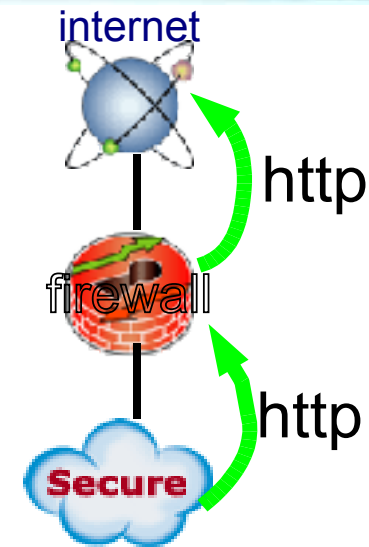
- Réunions de suivi et gestion des évolutions
 - Évolutions technologiques
 - Mises à jour des procédures de travail
- Audits par des tiers
 - Revue de résultats
 - Mises en place de mesures
- Réunions de bilan
 - Mises à jour contractuelles

- Comment allez vous gérer les journaux ?
 - Faire des corrélations et les analyser ?
 - Ou simplement les reformatter et me les renvoyer ?
- Quelle cohérence entre ce qui est infogéré et ce qui ne l'est pas ?
- 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 d'infogérance ?

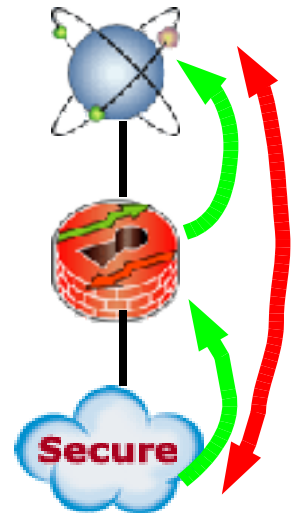
- Le système d'information est inter-pénétré de part et d'autre par les infogérances et les télémaintenances
- Relation contractuelle entre prestataire et client
- Exemples en télémaintenance
 - Routeurs chez les opérateurs de télécommunication
 - PABX
 - Imprimantes, télécopieurs, photocopieurs
 - SAN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

- Usage de liaisons téléphoniques pour contourner la sécurité périmétrique du firewall internet
 - Photocopieurs, SAN
- Usage de connexions HTTP/HTTPS pour contourner la politique de sécurité
 - Imprimantes
 - Assistance et support des applications en général
 - Prise de contrôle à distance des postes de travail des salariés
 - A l'insu de la DSI

- Laisser ouvert HTTPS sur Internet revient à connecter son réseau privé sur Internet sans *firewall*
- Il faut analyser le contenu de HTTP et d'HTTPS
- Rechercher les protocoles re-encapsulés interdits
- Analyser tous les contenus pour y détecter ceux qui sont malveillants ou ne répondent pas à sa politique de sécurité
- Appliquer le même filtrage dans HTTP que celui que nous réalisons sur TCP/IP dans les années 1990
 - Dans les deux sens



- Exemple de logiciels cherchant à contourner le contrôle d'accès du firewall :
 - Microsoft avec RPC over HTTPS, Outlook 2003, etc
 - VPN-SSL, ssltunnel, stunnel, http-tunnel, etc
 - Courrielweb (Webmail)
 - Logiciels d'EDI avec XML qui remettent du MIME et des protocoles de RPC dans HTTP/HTML,
 - Logiciels de messagerie instantanée
 - Logiciel de partage d'agenda et de messagerie
 - Logiciels basés sur les Web Services
 - Logiciels poste à poste (P2P:Peer-toPeer)



- Filtrer les logiciels de contournement de firewall institutionalisés
 - Logiciels volontairement installés sur le PC
 - Messageries universelles qui renvoient la messagerie d'entreprise à l'extérieur sans serveur central dans votre SI
 - Ipracom, Blackberry
 - Logiciel de prise de contrôle à distance
 - WebEx, Interwise
 - Téléphonie propriétaire
 - Skype
- Filtrer les logiciels malveillants qui sont passés à l'intérieur et qui recherchent la sortie vers l'extérieur
 - *Spywares, keyloggers, etc*

- La majorité des logiciels pilotent Internet Explorer
 - Il faut à la fois un *firewall* HTTP/HTTPS sur le périmètre et un *firewall* personnel sur chaque poste qui sachent travailler de concert
- Journaliser le trafic
 - Y compris le nombre d'octets transmis et les valeurs du champ Content-Length
- Détecter les anomalies et les valider / invalider
 - Beaucoup de trafic sortant
 - Site unique, URL unique
- HTTPS : autoriser les sites dans une liste blanche
 - Compromis à faire...

- Appliquer sa politique de sécurité
- Intégrer la sécurité dès le départ dans tout processus de télémaintenance
 - Contractuellement, systématiquement, ne serait-ce que pour savoir qu'il y a de la télémaintenance
 - De manière explicite
- Minimiser les télémaintenances au strict nécessaire
- Toujours les contractualiser

- Créer un portail de contrôle d'accès
 - Indépendamment des moyens de connexion
 - Authentifier individuellement chaque télémainteneur
 - Ouvrir le flux après l'authentification réussie
 - Journaliser les connexions
 - Recopier si possible la session complète des informations qui remontent à l'extérieur
- L'expérience montre que les fournisseurs commencent à accepter

- A l'usage, très difficile de faire coller l'offre standard au SI de l'entreprise
 - La politique de sécurité est éprouvée, mais l'infogéreur à un paquetage qui ne colle pas
 - Il propose quelque chose "d'équivalent", mais qui finalement dégrade un petit peu, et de fil en aiguille cela n'applique plus du tout la politique de sécurité

- Cas de l'accès au SI via un VPN chiffré :
 - Aucun opérateur ne couvre le périmètre
 - Besoin d'un courtier d'opérateurs
 - Besoin de déclarer, gérer, supporter et effacer chaque utilisateur dans plusieurs bases de données
 - Plusieurs couches d'authentification
 - Il faut refaire une authentification dans son SI avec son système de quarantaine en plus du système de l'opérateur
 - Problème avec les utilisateurs qui appellent leur support interne à l'entreprise et pas celui de l'infogéreur

- Cas de l'accès au SI via un VPN chiffré (suite) :
 - Nombreux problèmes techniques
 - Relayage radius
 - Incompatibilités Windows
 - Dialer windows ne supportant les authentification fortes
 - Problème de désynchronisations des clés
 - Usine à gaz sur chaque poste client qui devient ingérable
 - Nombreux problèmes organisationnels
 - Synchronisation lors des mise à jour des infrastructures
 - "Finalement nous n'avons toujours pas réussi à délimiter qui fait quoi au bout d'un an"

- 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

Questions ?

Herve.Schauer@hsc.fr

- **Conférence 7799 le 24 mai**

- <http://www.issafrance.org/premiere.htm>



- **Convention Sécurité les 15 et 16 juin**

- Exposition porte de Versailles
- Deux jours de tutoriels et de **conférences gratuites**
- Progr : http://www.hsc.fr/conferences/csm05_programme.html
- Inscription en ligne : <http://www.conventionsecurite.com/>



- **Formations SecurityCertified**

- Du 5 au 9 septembre et du 19 au 23 septembre
- Permettant de passer la **certification SCNP**
- <http://www.hsc.fr/services/formations/>



- Comment choisir son fournisseur de services d'infogérance en sécurité ?
 - Hervé Schauer, HSC, Le Guide de la Sécurité des Systèmes d'Information et Internet, février 2002
 - <http://www.hsc.fr/ressources/articles/infogérance/>
- Fournisseurs de Services en Sécurité, Comment les utiliser ?
 - Hervé Schauer, HSC, Eurosec 2002, Paris, 02/02
 - <http://www.hsc.fr/ressources/presentations/eurosec02/>
- Managing Technology Risk for IT - Service Provider Relationships
 - BITS working group from the Financial Services Roundtable
 - <http://www.bitsinfo.org/downloads/Publications%20Page/bits2003framework.pdf>

- Sur **www.hsc.fr** vous trouverez des présentations sur
 - Infogérance en sécurité
 - Sécurité des réseaux sans-fil
 - Sécurité des SAN
 - Sécurité des bases de données
 - SPAM
 - BS7799
 - etc
- Sur **www.hsc-news.com** vous pourrez vous abonner à la **newsletter HSC**