

COMMENT CHOISIR SON FOURNISSEUR DE SERVICES D'INFOGÉRANCE EN SÉCURITÉ ?

S'ils peuvent regrouper des activités diverses, tous les fournisseurs de services d'infogérance de services en sécurité (Managed Security Services Providers, MSSP) assurent cependant la gestion et la surveillance de périphériques ou systèmes. Cela peut être via l'infogérance de firewalls, la centralisation et le traitement des journaux, l'infogérance de logiciels de détection d'intrusion, les tests de vulnérabilités, l'infogérance de VPN chiffrés, l'infogérance d'antivirus, l'hébergement d'infrastructure de clés (PKIs) ou de services d'authentification des utilisateurs, notamment pour des accès distants avec des serveurs Radius. Ils peuvent aussi gérer la sécurité de l'hébergement de serveurs Web ou de plates-formes de commerce électronique. Dans le cadre de plans de continuité d'activité, il est aussi possible de prévoir une infogérance en cas de défaillance des services de sécurité d'une entreprise.

L'intérêt des entreprises et organisations pour l'infogérance en sécurité s'explique par la possibilité d'économies en terme financier, celle de bénéficier d'un service 24h/24h en évitant d'avoir ses propres centres d'exploitation des équipements de sécurité, ou, tout simplement, par la capacité de maintenance et d'amélioration de la sécurité déjà existante. Les infogéreurs en sécurité leur sont également nécessaires en raison de facteurs plus profonds : si un réseau est infogéré, il devient parfois difficile d'en garder la gestion de la sécurité. Il faut aussi prendre en compte le fait que les systèmes gérant principalement de la sécurité se sont multipliés : le firewall sur son périmètre est aujourd'hui remplacé par une multitude de firewalls répartis partout, pour des applications diverses, constituant la base de l'application de la politique de sécurité. Les accès distants aux réseaux de l'entreprise passent par Internet et offrent accès à tout ou presque du réseau privé, la messagerie interne, par exemple, étant désormais accessible depuis un butineur dans un hôtel ou un cybercafé. Les VPNs chiffrés se multiplient, les plates-formes de commerce électronique aussi. La surveillance, pourtant fondamentale, est généralement le parent pauvre des ressources alloués, et l'analyse des journaux est insuffisante, voire inexistante, sans parler de la manière avec laquelle la détection d'intrusion est gérée.

Ce manque de personnel qualifié pousse aussi à l'infogérance : il devient difficile de suivre tous les projets pour y intégrer la sécurité dès le départ, et plus généralement de se focaliser sur ce qui est important. Ce manque de temps implique donc la sous-traitance, en espérant y trouver une meilleure industrialisation des processus, une meilleure information avec, par exemple, des procédures d'application rapide et globale des correctifs de sécurité. L'infogérance s'apprend, mais ce n'est pas une tâche facile et cela demande de l'expérience. Par conséquent, il convient plutôt d'infogérer la sécurité en dernier. Sachant qu'il ne faut sans doute pas infogérer de la sécurité sans expérience préalable significative dans ce domaine.

Le manque de maturité du marché en France est également problématique. Ainsi, le concept d'infogérance est moindre dans notre culture que dans celle des pays anglo-saxons. Beaucoup de fournisseurs de type MSSP ou ASP (Application Service Provider) sont des start-up ayant concentré les investissements du capital-risque en sécurité en 2000 et 2001, qui ne sont pas à l'équilibre financier et dont la santé demeure fragile.

Pour y voir clair, voici quelques acteurs classés à titre illustratif, la liste n'étant pas exhaustive. Les sociétés de conseil proposent de l'infogérance en sécurité, comme HSC avec le service des tests de vulnérabilité semi-automatiques récurrents, ou les " Big Five " : Accenture, Andersen, D&T, E&Y, KPMG, PWC. Ils ont souvent des partenariats. Ils proposent cependant directement de nombreux services d'infogérance en sécurité aux Etats-Unis.

Les intégrateurs, à qui il arrive aussi de signer des partenariats, sont de plus en plus nombreux à intégrer l'infogérance : Alcatel, Integralis, RISC, Telindus/CF6, Thales (Experlan, Global-Control, Neurocom), Ubizen, Via Networks, etc. Certains d'entre eux créent parfois une société commune avec un opérateur de télécoms pour faire de l'infogérance : par exemple Telindus avec Telecom Italia.

Les SSII (ATOS, Bull, Integris, Cap Gemini, EDS, Steria, etc.) ont souvent développé d'importants départements d'infogérance, et donc des offres d'infogérance en sécurité. Elles bénéficient donc de la structure et de l'organisation pour en faire, même si elles rencontrent parfois des difficultés à appréhender la problématique sécurité des technologies Internet.

Les start-up, souvent en mode ASP, sont plus concentrées sur un type de service : l'analyse des journaux pour Counterpane, les tests de vulnérabilité pour Intexxia, Intranode et Qualys, et l'infogérance de tunnels chiffrés pour Neoteris, Netcelo, Openreach et Smartpipes. Même dans cette catégorie, plusieurs entreprises n'ont pas l'infogérance de la sécurité comme seul métier.

Les éditeurs de logiciels de sécurité infogèrent principalement leurs propres produits tout en développant des offres globales sur cette base. Ainsi, ISS, NAI, Symantec, Trendmicro, etc. étendent leurs prestations en développant une activité de service, et en profitant de l'antivirus, plus facile à infogérer par son éditeur que par un tiers.

Dans certains cas, les vendeurs de plates-formes et d'équipements matériels (Compaq, HP, IBM, Nortel et Sun) ont aussi développé des offres de services d'infogérance en sécurité. Ils développent aussi des partenariats pour certains services.

Enfin, de nombreux fournisseurs télécoms et de services d'accès à Internet disposent d'une offre d'infogérance en sécurité, eux aussi en développant parfois des partenariats : BT, Cable & Wireless (ISDnet), Cegetel, Colt, France Télécom avec les services issus de Transpac, Equant, Olean et Wanadoo, UUnet, etc. Certains, notamment dans les pays anglo-saxons, ont acquis des procédures formelles tandis que d'autres, même s'ils maîtrisent la technique, restent plus artisanaux.

Des acteurs majeurs n'ont pas été cités, mais cela ne signifie pas qu'ils sont absents de ce marché. Ainsi, Cisco, par exemple, est présent au travers de ses investissements financiers dans des projets d'infogérance en sécurité.

Pour clarifier comment s'y prendre pour choisir une bonne infogérance des services en sécurité, huit phases successives sont indispensables, les sept dernières étant inspirées de la présentation " Technology Risk Management for Outsourced Relationship " de Faith Boetger, de l'association BITS, effectuée lors de la conférence RSA 2002.

1/ Décision de faire de la sécurité

L'infogérance ne résout pas la sécurité en elle-même, il faut d'ores et déjà avoir une politique de sécurité préalablement déployée qui devra être appliquée par l'infogéreur. Il faut qu'il y ait donc à la base une prise de conscience de la sécurité par les responsables de l'entreprise : PDG, directeur informatique, directeur financier, etc. Certaines directions pensent avoir délégué la sécurité au RSSI, mais elles doivent réaliser que cela est de leur responsabilité et se poser ces questions basiques mais fondamentales : 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 ?

A partir de là, si la sécurité n'est pas le cœur de métier ou si la sécurité impose une surveillance 24h/24 ou si je ne suis pas en mesure d'avoir le personnel adéquat, il sera possible de décider sereinement des choix pouvant impliquer de l'infogérance. Le RSSI devra quant à lui analyser la charge de travail de chacun, en plus de la sienne, pour garantir la réussite, et éviter les a priori sur l'infogérance.

2/ Décision de faire appel à l'infogérance

Il faut définir les objectifs en termes de métier et de résultats attendus indépendamment des technologies employées, puis lister les technologies utilisées ou souhaitées pour répondre aux résultats attendus. A partir de là, il faut choisir quelles technologies seront d'abord mises en infogérance, par exemple ce que l'on ne sait pas faire et qui est facile à sous-traiter, comme les tests de vulnérabilité sur son périmètre. Mais ce n'est pas parce qu'il est facile d'"outsourcer" ces tests qu'il faut les utiliser. Il faut qu'ils fassent partie intégrante de l'application de la politique de

sécurité. En effet, il y a 80 accès externes répartis sur la planète qui ne peuvent être audités sur place régulièrement. Il est donc préférable de les sous-traiter plutôt que de faire soi-même les tests.

De manière générale, les tâches répétitives et faciles à industrialiser seront plus faciles à infogérer, comme la gestion des firewalls et des VPN IPsec. Il faut comparer ce que l'on peut faire soi-même par rapport à ce que propose l'infogéreur. Par exemple, dans un test de vulnérabilités, il est possible que 95% des informations fournies ne soient d'aucune utilité dans son contexte. Il ne faut pas alors considérer que l'infogéreur en fait vingt fois plus que soi. Il faut aussi analyser dans quelle mesure il sera possible de garder une surveillance en direct des équipements sans avoir à les gérer.

Il est aussi possible de démarrer en faisant un audit de l'existant ou une analyse de risques, mais normalement la maîtrise de l'existant devrait être suffisante. Enfin, quand la décision est prise, il faut lister les freins au succès de l'opération par rapport à une gestion en interne, et bien tout documenter par écrit avant de passer à la phase suivante.

3/ Fabrication d'un appel d'offres

Il faut bien définir le service souhaité dans l'appel d'offres : fonction, disponibilité, reporting, surveillance en direct, échelle et performance, gestion, suivi, etc. Préciser la sécurité choisie et décrire les techniques souhaitées, les moyens humains envisagés et le plan de secours souhaité.

4/ Analyse des propositions

L'analyse des propositions est proche de toute lecture de réponse à un appel d'offres : il faut prendre en compte l'expérience de l'infogéreur et ses références dans le domaine. Par rapport à la demande initiale, il faut vérifier que la réponse prend en compte l'ensemble des besoins actuels et à venir, contrôler s'il y a des dépendances à d'autres fournisseurs via des partenariats, et voir sa capacité à permettre des adaptations spécifiques dans une approche personnalisée. Il faut analyser ses méthodes de travail, les technologies utilisées et le personnel sur place : expérience, compétence, etc. La possibilité d'audits par des tiers sera très importante pour savoir ce qui se passe. Il convient de regarder ce qui est proposé et quel est le périmètre possible de ces audits : audits organisationnels et méthodologiques sur les procédures et le personnel ou audits techniques du centre opérationnel. Il est là aussi important de voir ce qu'il est possible d'auditer : ses serveurs et boîtiers seuls ou l'infrastructure mutualisée, uniquement les systèmes ou les applications avec le code source également, etc. Le choix des auditeurs agréés par les deux parties doit être précisé. Il faut aussi regarder si l'infogéreur prévoit, ou pas, l'accès de rapports d'audit d'un client à d'autres clients. La nature de la relation avec l'infogéreur dépend souvent du système de suivi et de surveillance : s'il faut sans cesse téléphoner, la relation risque d'être difficile. Elle sera meilleure si un système permet de voir par soi-même si un changement dans une règle de sécurité a été effectué, quand un VPN est tombé. Il faut aussi voir quels sont les mécanismes d'alarme et ce qui est proposé en cas d'incident, y compris sur le plan de la responsabilité et l'assurance.

5/ Accord sur les contrats de service

Le contrat est une synthèse de l'appel d'offres et de la proposition, avec une meilleure précision et exhaustivité, quitte à préciser des détails. Il doit inclure la description du service rendu, les rôles et responsabilités des parties, le renouvellement, la rupture et le transfert du contrat, vos méthodes d'accès au service infogéré, les méthodes d'archive des journaux, les conditions d'audit par un tiers et l'assurance. Le contrat doit être négocié et validé par le personnel compétent techniquement et le RSSI, et pas simplement par un juriste.

6/ Consensus sur les procédures de travail

Le travail semble souvent terminé une fois le contrat signé. Beaucoup de détails pratiques ne sont cependant pas contractuels et peuvent jouer comme facteurs de tension par la suite. Il faut donc avoir accès aux documentations et procédures de l'infogéreur, par exemple pour l'accès physique aux locaux, et documenter les dialogues et des détails comme la procédure de création et suppression de comptes, etc. Souvent les procédures en cas d'incident, de même que les responsabilités et le partage des tâches, pourront être détaillées dans un document de procédure de travail, ce qu'il était impossible de faire dans le contrat.

7/ Implémentation

Le projet d'implémentation demeure proche d'un projet d'intégration classique.

8/ Gestion de la relation dans le temps

La réussite de l'infogérance passe par des réunions de suivi et une gestion des évolutions technologiques, avec une mise à jour des procédures de travail régulière. Il faut y ajouter des audits par des tiers réguliers, au moins annuels, avec une revue de résultats et la mise en place de mesures adéquates si le besoin s'en fait sentir. Enfin, il peut être nécessaire de mettre à jour le contrat, notamment quand les résultats attendus et le périmètre changent. Une réunion annuelle de bilan est donc souhaitable.

En bref, le choix d'une société d'infogérance en sécurité dépend d'abord d'une bonne organisation interne de la sécurité, avec une politique dédiée et une direction consciente des enjeux et des responsabilités. Il convient ensuite de bien analyser (par rapport à ses besoins, ses moyens et son environnement) quel services infogérer et quels fournisseurs sélectionner, sans opter en fonction du prix mais plutôt en analysant le fond et le retour global sur investissement dans le temps.

Hervé Schauer

Hervé Schauer Consultants