Luc-François Salvador, Sogeti : « La cybersécurité, une activité qui croit de 30 % par an »

En amont du FIC 2014, le **Forum International de la Cybersécurité** qui s'ouvre demain à Lille, rencontre avec une des figures du secteur, **Luc-Français Salvador**, le patron de Sogeti. La SSII du groupe Capgemini a ces dernières années développé une activité cybersécurité, essentiellement tournée vers le secteur public et notamment vers les segments les plus sensibles de ce dernier (en particulier la Défense).

Principal partenaire du FIC 2014, Sogeti tente désormais de déployer cette expertise en direction des grands comptes et à l'international. La SSII est parvenue à attirer **Bernard Barbier**, l'ex-directeur technique de la DGSE, les services de renseignement extérieurs français, devenu le conseiller spécial de Luc-Français Salvador. Une expertise pointue particulièrement adaptée à l'heure où les grandes entreprises françaises cherchent à se protéger de la curiosité de la NSA américaine.

Silicon.fr – **Quel est aujourd'hui le positionnement de Sogeti sur la sécurité ?**

Luc-François Salvador – Sogeti, membre à part entière de Capgemini, est certes leader sur cette thématique au sein du groupe, mais cela n'a rien d'exclusif. Cette histoire a démarré il y a environ 5 ans de cela avec un manager, Edouard Jeanson, passionné par cet univers, qui a monté un petit laboratoire de R&D. Très vite, il m'a attiré dans ce monde il est vrai fascinant.

Grâce à des contacts avec les autorités françaises, nous nous sommes aperçus que cette R&D était de grande qualité. Et nous classait parmi les 4 ou 5 acteurs français principaux. A partir de là, ce qui était resté de la pure R&D est alors devenu une activité à part entière. Cette proximité avec les autorités du pays, que nous avons conservée, fait de Sogeti un acteur un peu à part. Nous sommes ainsi un des 5 prestataires labellisés de confiance par l'Anssi (Agence nationale de la sécurité des systèmes d'information). Le Cesti (Centre d'évaluation de la sécurité des technologies de l'information) auparavant situé au sein du CEA (Commissariat à l'énergie atomique, NDLR) nous a été cédé, ce qui nous permet de labéliser des niveaux de confiance sur des matériels et logiciels.

De l'extérieur, on a l'impression que Sogeti investit de plus en plus sur ce secteur…

C'est vrai. Même si ce sont des mondes qui demandent une certaine discrétion, bien que les choses tendant à évoluer notamment avec l'affaire Snowden. Nous étions naturellement discrets sur ces sujets d'autant plus que, sur cette activité, nous travaillons avec la Défense nationale, y compris sur des domaines très confidentiels.

Notre offre de service est basée sur une approche systémique. Nous savons, à très haut niveau, auditer et définir ce qu'est la situation de la sécurité d'une organisation, mettre en place un certain nombre de solutions matérielles ou logicielles et héberger nos clients sur nos SOC (Security Operations Center) de Toulouse ou Mumbai, pour la surveillance active de leur sécurité. L'ensemble

représente environ 300 personnes en France, dont 50 consultants de très haut niveau. Et s'insère dans notre réseau européen Sogeti. Au Luxembourg, par exemple, Sogeti a reçu l'agrément du gouvernement pour travailler sur la donnée bancaire, un domaine sensible dans ce pays.

Comment évolue le chiffre d'affaires de cette activité ?

C'est une activité en très forte croissance. La sécurité représente environ 30 millions d'euros (à 80 % dans le secteur public, NDLR), sur un total de 450 millions pour Sogeti. Mais elle connaît entre 20 et 30 % de croissance. Le vrai frein dans cette activité en France réside dans la ressource humaine. Les compétences de haut niveau sont rares, tous les acteurs se les disputent et l'Etat en attire beaucoup. Que ce soit la DGSE, l'ANSSI, la DGA ou la police.

En la matière, Sogeti vient précisément de réussir un coup en attirant Bernard Barbier, l'ex-directeur technique de la DGSE…

Bernard Barbier, que nous connaissons bien et depuis longtemps, va m'aider à construire une démarche encore plus internationale sur le sujet de la sécurité.

Lors du FIC, vous participez à une table ronde intitulée 'La cybersécurité est-elle un échec ?' S'est-on trompé de chemin ces dernières années ?

Déjà, il faut relever la vitesse d'évolution sur ces sujets. En France, les premiers éléments de doctrine émanant des autorités datent de 1994 seulement. En finalement peu de temps, quelque chose qui était annexe a pris une place centrale ; quel est le président de grande entreprise qui connaissait son RSSI voici seulement 5 ans ? Aujourd'hui, la sécurité informatique est devenue un sujet de conseil d'administration car on touche à la valeur immatérielle de l'entreprise. Regardez Sony : le vol du fichier clients ne se traduit par aucune perte financière directe pour la société, mais l'impact sur l'image est tel que l'action en a souffert. Conséquence : le RSSI est en train de migrer de la techno vers la gestion des risques.

Est-ce qu'on a commis des erreurs ? Certainement n'a-t-on pas pris conscience assez vite de l'importance de la menace que les cyber-attaques font peser sur les organisations. Les dernières affaires, en France ou à l'étranger, montrent l'étendue des conséquences. Rappelons qu'il y a seulement quelques années, on parlait plutôt d'une activité quasi-ludique : des hackers un peu Robin des bois qui tentaient de pénétrer les systèmes du Pentagone pour faire parler d'eux. Désormais, on assiste à des actes de malveillance émanant soit de criminels, soit si ce n'est d'Etats, au moins d'organisations para-étatiques. Quand on analyse l'attaque Shamoon sur la compagnie pétrolière Aramco, on décèle la patte d'un service secret.

Dans les grands pays, comme la France, cette prise de conscience est aujourd'hui avérée. Et c'est un des rares espaces où l'autorité publique, le régalien, a pris les devants. Avec, en France, par exemple l'Anssi ou la DGA, très active dans l'identification de cet écosystème très riche de petites sociétés françaises très en pointe sur ce secteur.

Est-ce que les révélations d'Edward Snowden, et surtout peut être leur récurrence, ont changé quelque chose ?

Evidemment. Ces révélations ont créé un choc dans l'opinion. Même si c'était évident pour les bons

connaisseurs de ce sujet. Le cyber-espace est un nouvel espace géostratégique, dans lequel le citoyen rencontre le consommateur, l'entreprise, l'autorité, etc. Et cet espace-là est animé par une technologie mise en œuvre dans une absence totale de régulation.

[Lire notre dossier : Tout sur l'arsenal secret des espions de la NSA]

Les derniers chiffres montrent une inflexion des mentalités. Aux Etats-Unis, 86 % des consommateurs Internet disent prendre des mesures pour masquer ou détruire leurs traces laissées sur le réseau. Plus de 70 % des internautes européens disent vouloir savoir où sont stockées leurs données et les contrôler. La Cloud Security Alliance a récemment sondé 500 dirigeants d'entreprise non américains ou ne résidant pas aux Etats-Unis. Près de 60 % d'entre eux affirment que la décision de la localisation de la donnée et de son contrôle devient stratégique.

Cela signifie que Amazon, Google et Microsoft – une large part du marché du Cloud aujourd'hui – vont soit devoir répondre très précisément à ces préoccupations, soit voir une partie du marché leur échapper. On est ici au-delà de la simple notion de sécurité, pour entrer dans ce que les anglo-saxons appellent le 'Trust & risk management', qui englobe la souveraineté de la donnée, la confidentialité des données, la gestion des identités…

Globalement, les fournisseurs de logiciels et de matériels de sécurité sont américains, la force de l'Europe résidant plutôt dans le service. Est-ce que la crise de confiance créée par les révélations d'Edward Snowden est susceptible de modifier cet équilibre ?

Prenons les différentes catégories de fournisseurs une par une. Le domaine des équipementiers est effectivement dominé par les anglo-saxons, mais il demeure un acteur franco-américain (Alcatel-Lucent) et un autre allemand (Siemens). Au-delà de Cisco et Juniper, quand on voit la vitesse à laquelle Huawei prend position, on peut clairement se dire que l'Europe n'a pas de réponse adaptée. On aurait pu imaginer un regroupement des grands équipementiers européens, autour d'Alcatel, de Siemens et de Nokia.

En matière d'intégrateurs et de sociétés de services, on peut distinguer deux familles. Les sociétés de grande taille, comme Capgemini, Cassidian ou Thales, où l'Europe est bien armée. Et toute une galaxie de petites sociétés vouées à rejoindre des structures plus importantes. Pour une raison simple : pour attirer les compétences, il faut avoir la reconnaissance du marché.

Enfin, existe tout un univers de logiciels ou de combinaisons de matériels et de logiciels, où évoluent de nombreux grands acteurs anglo-saxons, mais aussi russes ou chinois. En la matière, la France dispose d'un écosystème d'une grande richesse, par exemple sur le cryptage ou la PKI. Des sociétés souvent de petite taille qui sont appelées à se regrouper, même si elles ont parfois encore du mal à l'accepter. En la matière, l'Etat a d'ailleurs une vraie réponse via la création d'une filière des industriels de sureté. Sans oublier le rôle que tient la DGA, tant par ses budgets d'investissement que par ses réalisations. La technologie française a clairement un rôle à jouer dans le secteur. Elle a simplement besoin de se fédérer.

Il y a quelques années, le sujet clef était de bloquer les attaques massives de type DDOS. Aujourd'hui, on entend de plus en plus parler d'attaques ciblées, plus pernicieuses. Est-ce ce critère qui est devenu la clef pour gagner des contrats avec les entreprises du CAC 40 ?

Le sujet le plus grave aujourd'hui réside effectivement dans ces attaques qui passent inaperçues et qu'on découvre par accident. Prenons par exemple celle qui a frappé le ministère des Finances à Bercy ou celle qui a visé la Commission européenne. Dans les deux cas, la découverte de l'attaque a été accidentelle. On s'est aperçu que, en dessous même de la couche de système d'exploitation, étaient installés des programmes qui inspectaient, traitaient et éventuellement envoyaient à l'extérieur des données. Pour une grande entreprise se battant sur des marchés internationaux, le risque est de voir les informations concernant ses grands contrats espionnées et réutilisées par d'autres, d'assister au pillage de ses propriétés intellectuelles, de voir ses avantages compétitifs réduits à néant. Ensuite, il ne faut pas oublier une autre famille d'attaques, liées à la réputation de l'entreprise ou de ses dirigeants.

Quels sont les axes de développement de Sogeti dans la cybersécurité en 2014 ?

Déjà, nous souhaitons maintenir notre croissance autour de 30 %. Nous poursuivrons nos investissements sur notre SOC de Toulouse et sur nos alliances, notamment avec IBM et Microsoft. Et nous allons de plus en plus travailler sur la globalisation de la sécurité, avec les autres entités de Capgemini, afin d'accompagner les grandes entreprises de dimension mondiale. Cela peut passer éventuellement par la création d'une entité spécifique. Nous devons présenter des propositions en ce sens au comité exécutif de Capgemini avant la fin de premier trimestre.

En complément :

Toute l'actualité de la sécurité sur Silicon.fr