Divers

Organisation et sécurité: en finir avec le cloisonnement !

*Par **Bruno Vincent**, le 09 sept 2008 à 17:31:15 - Dernière modification le 18 sept 2008.*

DSI,RSSI et Métiers ont encore du mal à collaborer efficacement. Pourtant, l'organisation s'avère être, une fois de plus, la pierre angulaire d'un Système d'Information sûr et aux coûts maîtrisés.

Au printemps dernier, sur lesnouvelles.net, un RSSI s'en prenait dans **une carte blanche** aux « DSI réactives et bien pensantes » du monde bancaire, qui selon lui négligent les alertes des directions sécurité (notamment sur la partie réglementaire) et participent à une forme de gommage du mot « Responsable » dans l'acronyme RSSI. Ce sentiment - comme tous les sentiments - est bien entendu recevable. Pour autant, à la lecture du rapport 2008 du Clusif (Club de la Sécurité de l'Information Français) sur les "*Menaces informatique et pratiques de sécurité en France*", il ne semble pas être partagé par tous. Le rapport du Clusif rapporte en effet que seuls 8% des RSSI citent la réticence de la DSI comme un des principaux freins à leur mission. Alors ce RSSI se serait-il alarmé trop vite ? La sécurité a-t-elle trouvé dans le SI un foyer accueillant, prévenant et sensible à ses requêtes ? Assurément non ! Le malaise organisationnel existe bien, le rapport précisant effectivement qu'outre la problématique récurrente du budget, ces mêmes RSSI considèrent que ce sont les contraintes organisationnelles, la réticence de la hiérarchie, des services et des utilisateurs qui arrivent en tête des obstacles à surmonter.

S'il n'est donc pas centré sur la DSI, le ressenti n'en demeure pas moins avéré. Et au demeurant fort légitime car les conséquences sont loin d'être neutres ! Le rapport du Clusif relève en effet sur la période 2006-2008 un "*inquiétant sentiment de stagnation*" de la sécurité des SI. Le rapport souligne qu'après une période propice à la rédaction des politiques et des chartes de sécurité, peu de mises en application concrètes ont vu le jour, et ce, en dépit des retentissantes affaires de ces derniers mois (**Affaire Kerviel** à la Société Générale, **perte de données personnelles** au Ministère de l'Intérieur britannique, etc).

Alors, comment soulager ce ressentiment envers l'organisation ? En la décloisonnant ! Car c'est bien là la cause de nombreux maux. Ainsi, la situation décrite par ce RSSI dans sa carte blanche tient assurément plus de l'incompréhension mutuelle, que d'une mauvaise volonté assumée par l'une ou l'autre des parties. Cette incompréhension, alimentée par des différences d'objectifs, de cycles de vie et de livraison, se retrouve exacerbée par la distanciation des équipes et leur trop faible participation à des projets communs. De fait, nombreux ont été les RSSI ces dernières années, à diligenter auprès de la DSI et des Métiers, des correspondants sécurité chargés de recueillir les besoins des utilisateurs et d'insuffler aux projets les bonnes pratiques édictées dans les chartes. Si cette approche est profitable, elle n'est cependant souvent pas suffisante dans un domaine requérant des compétences aussi variées que l'analyse de risques, l'architecture applicative ou les infrastructures de production. Ainsi, elle ne répond pas, du moins pas intégralement, à la première demande des projets, à savoir la fourniture de solutions de sécurité packagées, rapidement intégrables dans leurs socles respectifs.

Face à ce manque, les entreprises - de même que les organismes publics et les collectivités locales - se laissent désormais tenter par de nouvelles formes d'organisation. Des cellules virtuelles, c'est à dire composées d'interlocuteurs rattachés à des services bien réels, mais dotées d'un budget propre, voient ainsi le jour. Ces comités sécurité, en quelque sorte en "*mode projet permanent*", regroupent des fonctionnels du métier, des architectes techniques, des correspondants du RSSI, des chefs de projets « phare » et visibles du SI avec une forte composante sécurité (ex: B2C, projet portail, ouverture du SI à l'international etc.) et parfois aussi des représentants de la production. Leur mission est triple :

- piloter l'exécution effective des schémas directeurs sécurité ;
- répondre aux questions et aux besoins des projets par des solutions packagées et adaptées aux risques ;
- communiquer auprès des services de la DSI, du RSSI et des Métiers sur l'avancement des travaux.

Certes, ces cellules collaboratives relèvent encore de l'innovation. Pour autant, les entreprises qui les testent, ou les déploient, participent autant à la sécurité de leur SI qu'à la rationalisation de ce dernier. Elles permettent en effet d'assurer une cohérence

CARTES BLANCHES

IAM : dépenser moins pour gagner plus
Bruno Vincent

Une phrase d'Eric Domage, d'IDC, interpelait récemment décideurs et acteurs du marché sur l'importance des coûts et le peu de ROI découlant des projets d'IAM. Bruno Vincent nuance voire réfute en partie, ces propos.

Organisation et sécurité: en finir avec le cloisonnement !
Bruno Vincent

DSI,RSSI et Métiers ont encore du mal à collaborer efficacement. Pourtant, l'organisation s'avère être, une fois de plus, la pierre angulaire d'un Système d'Information sûr et aux coûts maîtrisés.

Les RSSI du monde bancaire à l'aube d'une vague de démissions ?
Monsieur RSSI

Rien ne semble changer en matière de risques et sécurité dans le monde bancaire. Constat désabusé et inquiet d'un RSSI du secteur.

Rififi en vue chez les identités
Bruno Vincent

Alors qu'OpenID attise l'intérêt des géants de l'informatique, l'acquisition de Credentica par Microsoft laisse augurer d'une possible guerre des « standards » en matière de gestion des identités sur le Web.

>> Plus de Cartes Blanches

Les thématiques

Quel socle de connaissances pour le RSSI ?
Les services managés de sécurité à l'age adulte
Les botnets se mettent au Web 2.0
Antivirus : la révolution *in the cloud*

dans l'architecture des solutions, dans le planning, le positionnement respectif et la mise en œuvre des solutions et des projets. Enfin, et d'aucuns seraient tentés de dire « surtout », ces formes d'organisation renforcent, autour de la sécurité du Système d'Information, l'adhésion de services de natures ou de cultures souvent très différentes. L'analogie vaut ce qu'elle vaut mais aux vues des malaises qui freinent aujourd'hui la mise en œuvre pratique des politiques de sécurité dans les entreprises, on ne saurait que promouvoir le passage à cette « Sécurité 2.0 » !

A Propos de l'Auteur

Bruno Vincent est co-fondateur du cabinet de conseil ITekia, spécialiste de l'architecture, du pilotage et de la sécurité des Systèmes d'Information.

Diplômé de l'université britannique d'Aston et de l'Ecole Nationale Supérieure d'Informatique pour l'Industrie et l'Entreprise (ENSIIE), Bruno Vincent a débuté sa carrière chez EADS Sycomore, puis a rejoint le cabinet Octo Technology où il y a dirigé l'offre sécurité. En 2008, il cofonde ITekia et en assure la Direction Technique.

Bruno Vincent a coécrit l'ouvrage "*Gestion des Identités : Une Politique pour le Système d'Information*" et enseigne l'architecture de SI à l'Ecole Nationale Supérieure de Techniques Avancées (ENSTA).