Eurosec 2007 : Tous responsables, aucun coupable…

Pierre Auguste, RSSI de SFR, ouvre le bal : *« Il n'existe pas de définition type de mon métier*[Responsable de la sécurité du système d'information]*. Pour évoquer mon cas personnel sur le périmètre du système d'information, je préfère parler de fonction ou de mission plutôt que de métier. Ma mission se construit autour de quatre axes: -exécuter la politique de sécurité, -mettre en oeuvre les mesures techniques pour que l'infrastructure présente un niveau de sécurité satisfaisant. -mais j'ai aussi un rôle d'assistance ou de conseil; -enfin, le RSSI se porte garant de la politique de sécurité, il a un rôle de vigie, qui est détaillé dans sa mission. »*

« Chez SFR, le réseau à gérer est vaste, en conséquence, il y a également un directeur de la sécurité dont le métier est de surveiller toutes les facettes de ce périmètre. Il n'y a pas de DSI chez SFR. Je dispose de mon budget propre, j'ai donc les moyens de mettre en oeuvre l'assistance, la mise en place des solutions logicielles et matérielles, sans oublier les audits. Les sociétés disposent toutes de chartes de sécurité, ces dernières définissent le rôle du RSSI, mais il y a un facteur que l'on a tendance à oublier, ce sont les ***règles non écrites****, par exemple garantir le droit des salariés. Voilà donc la mission du RSSI, il y a un « grand patron sécurité au sein du groupe, puis, dans le SI, il y a une déclinaison des responsabilités. Selon les réglementations de l'entreprise, la responsabilité peut être éclatée. SFR est une structure centralisée. Dans l'organisation, s'il y a un problème, il y a 3 têtes sur lesquelles taper »*, poursuit Auguste.

*« La politique de sécurité est propre à chaque groupe, »*déclare Pierre Auguste*, « elle est réalisée de façon générique, et elle vise à définir les grands principes de responsabilité dans le domaine de la sécurité. Elle est constamment en évolution, et évoque l'existence du respect des obligations légales et réglementaires qui sont applicables à toutes les entreprises. Les grands principes qui régissent la politique de sécurité sont les suivants : protéger le patrimoine du groupe, et définir la responsabilité opérationnelle «* , ajoute-t-il.

Pour sa part, Philippe Tassin, DSI du Crédit immobilier de Paris estime : *« Quand ça ne marche pas, c'est à moi que l'on téléphone. En plus, dans le domaine financier nous sommes soumis à un audit de la Commission bancaire. Selon moi, le RSSI a une mission différente de celle du DSI. Sa fonction est de définir la politique de sécurité, la promouvoir, et surveiller la relation du groupe avec la CNIL et garantir la continuité de l'activité. Dans la pratique, il est souvent tout seul, cela est donc très différent. Quant à la question de savoir si sa responsabilité pénale peut-être engagée en cas de problème*[ndlr : fuite des données, espionnage industriel]*cela n'est pas clair et dépend de la société. Chez nous, c'est moi qui suis responsable, le RSSI fait parti de la direction informatique, mais il faut reconnaître qu'il existe de nombreux profils de RSSI. »*

« C'est vrai! », réagit Pierre Auguste : *» Le périmètre de responsabilité dépend de la taille de l'entreprise et de son approche de la sécurité. Par exemple, je suis personnellement responsable des réseaux et la sécurité ».*

Alors qui choisir entre RSSI ou DSI?

Interrogé sur ce points -RSSI ou DSI-, Godefroy de Bentzman, dg de Devoteam répond : *« De toute façon, le patron est toujours responsable. Je cherche l'efficacité, par conséquent il est important de ne pas se disperser. À mon avis, le fait d'avoir deux personnes dont les fonctions se croisent est relativement gênant. Personnellement, j'estime que le DSI est le responsable et que ses équipes de techniciens sont là pour l'aider. Pour être efficace, l'organisation de la sécurité doit être simple. »*

Autre avis, celui de Thierry Serres, DRH de Bouygues Construction commente: *« Au sein du groupe Bouygues il y a eu une véritable maturation du poste. Le premier RSSI a été nommé en 2002. Son travail est d'analyser les risques et les enjeux sous l'autorité du DSI. Puis d'établir une politique pour les risques informatiques. Il faut établir des règles puis définir un plan d'action. »*

Pierre Auguste de SFR précise : *« Il y a des programmes de sensibilisation, dans notre cas, nous présentons régulièrement à l'ensemble de nos collaborateurs, les règles de l'entreprise. Nous disposons d'une ligne d'assistance, 'hotline', et de sites Web spécialement dédiés à la sécurité. De cette façon, il existe une possibilité de faire remonter l'information en cascade. Je suis très clairement sous la tutelle du DSI; il a, lui, une responsabilité pénale. Il contrôle, il mène une veille juridique, et lance les audits. Il faut donc sensibiliser le personnel qui est le maillon faible de la sécurité. La politique de sécurité peut être et doit être partagée. »*