Tribune : 'Fraude' à la Société Générale, génie isolé ou insouciance généralisée ?

Le plus gros : Kerviel a usurpé « des codes d'accès informatiques appartenant à des opérateurs pour annuler certaines opérations ». Cela veut dire qu'il a conservé d'anciens mots de passe ? Qu'il en a obtenus ? Qu'il s'est fait passer pour ces opérateurs qui auraient dû voir quelque chose ! A moins que lesdits opérateurs ne puissent voir ce que l'on fait en leur nom ? À moins qu'ils ne soient plus en poste ?

Dans tous les cas de figure, il y a là une très mauvaise gestion des login et une sensibilisation très insuffisante des intéressés à la sécurité. Et un contrôle absent. Trouver cette situation dans une grande banque française est surprenant. La préoccupation de la sécurité doit amener la hiérarchie à sensibiliser en permanence sur ces points : il y a là un manquement grave de la hiérarchie. Par ailleurs, il est très étonnant que les audits n'aient rien vu… cela peut laisser penser que ces manquements à la sécurité sont absolument courants.

Deuxième point surprenant : le trader aurait justifié certaines opérations fictives « en falsifiant des documents » dont on peut penser que certains sont des courriels. Etant donné l'importance de ces envois, il est surprenant de constater qu'ils ne sont pas protégés dans un système de dépôt sécurisé. Là encore le contrôle ou les audits se contentent de vraiment peu ! Il est donc possible de se justifier avec un courriel trafiqué ?

Troisième point un peu plus subtil tout de même : il semble que Kerviel connaissant bien les contrôles se soit glissé dans les failles. Faut-il en déduire que ces failles n'étaient pas connues des auditeurs ou contrôleurs ? Des failles minimes et peu risquées, passe encore ; mais des failles à 50 milliards d'Euro d'exposition ? L'analyse de risque n'est pas correcte ! A-t-elle seulement eu lieu ?

Enfin, il semble que le contrôle ne soit pas systématique sur toutes les opérations, mais plutôt statistique ou sur les opérations les plus courantes ou les plus grosses financièrement. Le compromis entre le risque et la complétude du contrôle est toujours difficile à trouver, mais dans le cas qui nous préoccupe, il est très défavorable !

Pour finir, la page 5 du communiqué donne un renseignement important : » la position [de la banque] sur futures a été rapprochée de la position de notre contrepartie (compensateur) », ceci, afin de s'assurer que toutes les opérations fictives ont été identifiées. Cette phrase indique donc qu'il existe un moyen externe et 'holistique' de contrôle qui visiblement n'a pas été utilisé jusque là.

Sans préjuger des torts de Kerviel, on peut dire à la lecture de ce communiqué que l'analyse des risques liés à l'usage de l'informatique est très insuffisante dans cette banque. La politique de sécurité et la préoccupation de son maintien auprès des utilisateurs de l'informatique est aussi déficiente. Partant de là, les contrôles et audit passent à côté de la réalité opérationnelle. C'est un retour aux vrais risques informatiques qui doit s'opérer avant tout, car sans informatique de base sécurisée, tout n'est qu'illusion.

___

(*) Consultant, Duquesne Research