Gwenaël Letellier (Intrinsec): «Le RGS va redonner la parole aux DSI»

Ordonnée en 2005, décrété le 18 mai 2010, le référentiel général de sécurité (RGS) *« s'impose aux autorités administratives pour les systèmes d'information dans le cadre des échanges d'informations soit avec une autre autorité, soit avec les usagers lors des transactions en ligne (paiement, inscription, formulaires, etc.)*, explique Gwenaël Letellier, responsable de l'offre RGS chez Intrinsec. *L'objectif est d'assurer la disponibilité du système d'une part, et l'identification et authentification des utilisateurs d'autre part »*. En d'autres termes, le RGS vise à renforcer la sécurité des échanges issus des services administratifs et, donc, instaurer la confiances des usagers. Au même titre que le RGI (référentiel général d'interopérabilité), le RGS participe au plan de modernisation de l'administration électronique.

Fondé en 1995, et filiale du groupe Neurone depuis 1999, Intrinsec s'est spécialisé dans le conseil en sécurité des SI et l'infogérance. L'entreprise a eu l'occasion de travailler avec de nombreuses entités administratives (conseil généraux, régionaux, ministères, municipalités, collectivités…), ce qui la met en bonne position pour aborder le marché du RGS à travers une offre en trois axes (diagnostique, accompagnement de projet pour les nouvelles applications et mise en conformité). Un marché au potentiel important puisqu'il concerne toutes les entités administratives même si *« beaucoup de clients se manifestent mais peu font la démarche »*.

Pour l'instant. Car les événements risquent de se précipiter. Selon le calendrier fixé, les administrations concernées disposent de 3 ans pour appliquer le RGS sur les applications mise en fonction avant le 18 mai 2010 et de un an seulement pour celles mise en route entre le 18 mai et le 18 novembre. Au-delà, toutes les applications nouvelles doivent être conformes au RGS.

« L'idée n'est pas de sécuriser à outrance. »

Ce qui laisse peu de temps aux administrations quand on sait qu'un simple test d'intrusion peut nécessiter jusqu'à un mois de travail. Un calendrier temporisé par la possibilité de délivrer des certificats temporaires. *« L'homologation temporaire peut être décidée s'il y a un écart entre les objectifs fixés suite à l'analyse et la mise en œuvre des applications*, nuance le responsable.*Le refus de mise en production reste réservé aux cas graves comme, par exemple, la possibilité d'accéder à la base de données en changeant un caractère de l'URL. »*

La mission d'Intrinsec se situe donc dans l'analyse du SI et le conseil, ainsi que dans la préparation du dossier à présenter pour homologation. *« Intrinsec intervient uniquement au niveau de la présentation du dossier de sécurité pour l'homologation, nous sommes vraiment sur l'accompagnement »* Homologation validée… par l'autorité administrative qui s'y soumet. Une démarche étonnante où le juge est forcément partie prenante de l'affaire. *« Si une organisation fait preuve de mauvaise foi lors de l'identification de l'application à homologuer, elle risque de se retrouver avec une homologation non conforme, effectivement. Mais les recommandations de l'ANSSI* qui a rédigé le RGS sont claires »*, temporise Gwenaël Letellier. Et *« L'idée n'est pas de sécuriser à outrance. »*

Le rôle d'Intrinsec, pour sa part, va au-delà de l'audit et du conseil. *« Nous sensibilisons à la sécurité les acteurs de la direction informatique et les responsables métiers, nous apportons la structure d'homologation, et préparons l'intégration des la gestion de la sécurité dans le workflow de gestion de projet, à quel endroit faire intervenir les intervenants, etc. »*, témoigne notre interlocuteur dans le cadre de la mise en oeuvre du RGS pour le Conseil général de Manche.

Portails web non développés dans les règles de l'art

Une démarche de sensibilisation qui a notamment permis à la DSI du Conseil de reprendre la main sur les choix applicatifs dont les applications métiers étaient décidées sans concertation avec les responsables du systèmes au risque de (trop) souvent négliger les aspects liés à la sécurité. *« Le souci étant souvent que les DSI agissent comme fournisseurs de contenant et pas sur les contenus. A ce titre, le RGS va redonner leur mot à dire aux directions informatiques. »*

Mais quels sont les points aujourd'hui sensibles concernés par le RGS? *« Les risques les plus récurrents se retrouvent dans l'absence des mises à jour de sécurité systèmes et applications, et des portails web non développés dans les règles de l'art de la sécurité (sensible aux injectionsSQL par exemple) qui répondait à des besoins à l'origine mais plus adaptés aux environnements actuels »* mis en lumière avec l'ouverture au web des applications. Si le RGS n'impose aucune solution, il oriente fortement vers l'authentification des utilisateurs, qui passe le plus souvent par la certification numérique au lieu du traditionnel login/mot de passe.

La sécurisation des échanges au sein des administrations est donc en route. A ce titre, et même si le décret a mis 5 ans avant d'être rédigé (ce qui oblige à rattraper le retard et accélère soudainement la mise en place du GRS), la sécurité des organismes publics *« n'est pas en retard par rapport entre ce qu'on rencontre dans le privé »*, estime Gwenaël Letellier. De là à dire que le RGS pourrait également concerner les entreprises privées…

** Agence nationale de la sécurité des systèmes d'information.*