par Isabelle Pottier

L'analyse de risque en matière de données personnelles et sensibles n'est pas une analyse classique

Jean Olive, senior manager au sein de CGI Business Consulting (*)

Pouvez-vous nous dire en quoi consiste votre activité au sein du Groupe CGI ?

CGI Business Consulting est le Cabinet de conseil du groupe québécois CGI spécialisé dans les services en technologies de l'information et de la communication. Pour ce qui est de la sécurité des systèmes d'information, nous disposons en France d'une équipe dédiée à l'assistance à maitrise d'ouvrage. C'est ce qui nous permet d'intervenir sur tout le cycle de vie des projets sécurité des SI, aussi bien en amont (conception, conseil) qu'en aval (mises en œuvre, audits, tests). Depuis 20 ans, j'assiste de nombreux organismes publics et privés dans la réalisation d'analyses des risques dans des domaines métiers variés. Et aujourd'hui, au sein de CGI Business Consulting, je suis responsable des prestations de conseil en sécurité des SI pour le compte du secteur public.

Y a-t-il une différence entre une analyse des risques « données personnelles » et « entreprise » ?

Oui. En matière d'analyse des risques portant sur les données à caractère personnel, il a une chose importante à retenir : il s'agit d'étudier les scénarios susceptibles de provoquer des préjudices aux personnes concernées et non pas une étude visant la protection des intérêts de l'entreprise. Deux séries d'obligations majeures figurant dans la loi Informatique et libertés orientent la démarche : l'obligation d'assurer la sécurité des traitements d'une part, et le respect des droits des personnes d'autre part (opposition, rectification, suppression, accès). Pour aider les responsables de traitements dans la conduite de ces analyses, la Cnil a mis en place deux outils simples : un guide ainsi qu'un catalogue de 55 mesures de sécurité génériques. Ce guide est une application particulière de la méthode EBIOS 2010(*). Le catalogue quant à lui, ne doit pas être pris comme un référentiel de conformité obligatoire, mais comme des bonnes pratiques que le responsable de traitement devra sélectionner, voir compléter, au regard des risques qui pèsent sur la vie privée des personnes.

Avec le projet de règlement européen visant à réformer la protection des données à caractère personnel, l'analyse des risques sera rendue obligatoire, ce dès la conception des projets (*Security by Design*). Ainsi, pour les projets en cours, il convient d'ores et déjà d'anticiper l'entrée en vigueur du règlement. Les autorités administratives qui échangent des informations entre elles et avec leurs usagers (téléservices) ont déjà l'habitude de cette démarche rendue obligatoire par le Référentiel Général de Sécurité (RGS) homologué.

En tant que cofondateur du Club EBIOS et auteur du logiciel éponyme distribué par l'ANSSI(*), pouvez-vous nous dire ce qu'EBIOS apporte à l'étude d'impact ?

La méthode consiste en une décomposition du risque : d'un côté les évènements que le risque provoquerait et de l'autre les failles qui le rendent possibles. Nous distinguons ainsi : la source du risque (origine accidentelle ou malveillante), les vulnérabilités du SI (dysfonctionnement de l'application, écoute du réseau, accès non protégé au serveur, etc.), la nature des données vulnérables et les conséquences du risque sur la vie privée des personnes. Cette décomposition vise deux objectifs principaux : 1) apprécier la vraisemblance de survenance du risque et sa gravité (les données sont-elles échangées en clair ? Quel est l'impact sur les personnes en cas de vol ?) ; 2) agir sur le risque à plusieurs niveaux pour le réduire (ex : réduire les données collectées, chiffrer les données pour ne plus les rendre identifiantes, protéger les accès pour éviter les vols).

Le projet de règlement européen rend obligatoire l'évaluation préalable de l'impact du traitement envisagé sur la protection des données personnelles, sous peine de sanctions financières lourdes. Nous apportons notre expérience de la conduite de cette démarche, notre expertise des failles et menaces en matière de sécurité des SI et notre parfaite connaissances des moyens de couvrir les risques y afférents.

(*) EBIOS® : Expression des Besoins et Identification des Objectifs de Sécurité est la méthode de gestion des risques publiée par l'ANSSI du Secrétariat général de la défense et de la sécurité nationale (SGDSN). Marque déposée SGDSN.