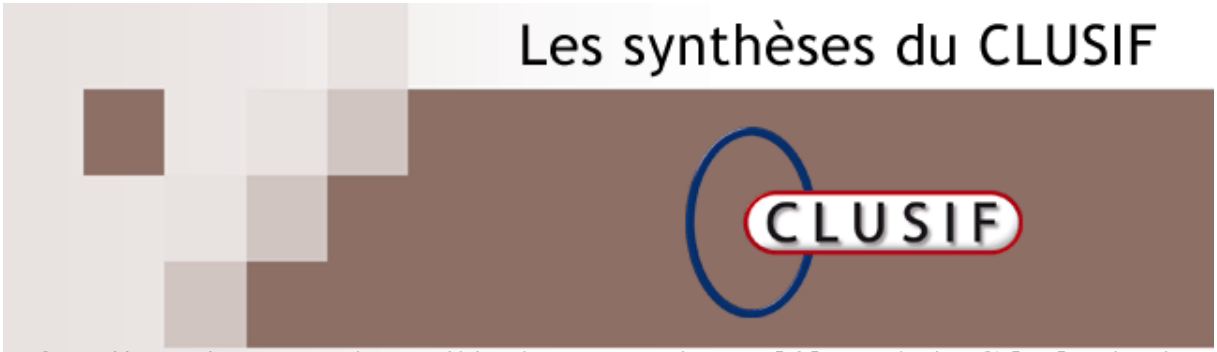

Quelle place aujourd'hui pour le Référentiel Général de Sécurité (RGS) ?

Synthèse de la conférence thématique du CLUSIF du 24 octobre 2013.

A quelques mois de l'arrivée de la version 2.0 du RGS (Référentiel Général de Sécurité), le CLUSIF a souhaité faire un état des lieux de la mise en application de la loi de 2005 (arrêté du 18 mai 2010) qui définit les règles de sécurité s'imposant aux autorités administratives dans la sécurisation de leurs systèmes d'information. Ce RGS propose également des bonnes pratiques en matières de SSI, que les autorités administratives sont libres d'implémenter.

Dans ce contexte de mise en application, le CLUSIF a souhaité partager son expérience lors de la conférence du 24 octobre 2013. Sept intervenants ont partagé leurs expertises et retours d'expérience : Lazaro PEJSACHOWICZ (CLUSIF), Frédéric DUFLOT (ANSSI), Raphaël MARICHEZ (Ministère de l'Intérieur), Jean-Noël OLIVIER (Mairie de Bordeaux), Benjamin LEROUX (Advens), Sébastien HERNIOTE (AMOSSYS), Hervé SCHAUER (HSC) et, en animateur de la table ronde, Jean-Marc GREMY (CLUSIF).

En tout premier lieu, le RGS c'est d'abord un « état d'esprit » – Par Lazaro Pejsachowicz

Au-delà de sa mise en application, le RGS est une avancée en matière de SSI quant à son esprit et quant à sa démarche unique. Grâce au RGS, les autorités prennent leurs responsabilités vis-à-vis de la protection des citoyens dans le cadre de leurs échanges électroniques. Si on considère que le RGS est la bonne approche de la SSI, fort de son succès et suite aux retours d'expériences de sa mise en application, la question de la mise en œuvre de cette démarche par les entreprises du secteur privé prend désormais tout son sens.

Le RGS : objectifs, défis et perspectives – Par Frédéric Duflot

L'objectif initial du RGS a consisté à créer un environnement de confiance et un cadre législatif en matière de dématérialisation et d'échanges numériques entre les autorités administratives et les usagers, ainsi qu'entre les autorités administratives elles-mêmes. Le RGS est le fruit d'un travail commun entre l'ANSSI et la Direction Générale de la Modernisation de l'État (DGME). Le RGS impose trois grandes obligations : mener des analyses de risques, mettre en place les mesures de sécurité pour homologuer les systèmes avant leur mise en exploitation et en dernier lieu, utiliser des produits et services qualifiés.

Le RGS fait face à de nombreux défis. À court terme, sa mise en œuvre devra être améliorée, et ceci dans des contextes très différents : des grands ministères aux collectivités territoriales. Pour ce faire, la version 2.0 proposera de qualifier les produits et services sur une durée plus longue, d'augmenter l'offre du catalogue de produits homologués et, en dernier lieu, de qualifier les prestataires d'audit de

sécurité du SI (PASSI)[1]. À moyen terme, le RGS devra anticiper les nouveaux enjeux tout en répondant aux enjeux existants et aux moyens mobilisables que soit par petites communes ou par les grands ministères.

Le RGS pour une prise en compte de la sécurité par tous, équilibre entre la gestion des risques et la conformité – par Raphaël Marichez

Au sein d'une autorité administrative la démarche d'**homologation** est une approche par la gestion du risque, via l'utilisation d'une méthode d'analyse des risques, pouvant être de type EBIOS ou autre. Cette démarche intégration de la SSI dans les projets les plus sensibles, consiste à faire porter ces risques par des AQSSI[2], à motiver les directions « métier », et enfin, à contrôler l'application des exigences de sécurité. Ce processus d'homologation n'est pas décrit par le RGS, c'est une « transposition interne ». Enfin, il doit être prolongé d'un comité de suivi (de type SMSI).

La mise en place des **briques de confiance** implique de recourir à des produits de sécurité et à des prestataires de services de confiance (PSCo) ayant fait l'objet d'une qualification. Enfin, **l'ouverture aux partenaires** est un pas vers la convergence des SI et l'interopérabilité de ces briques de confiance.

Une opportunité pour la sécurité au sein des collectivités territoriales – Par Jean-Noël Olivier et Bejamin Leroux

Le RGS est souvent associé à la mise en place de certificats électroniques et aux services de confiance. Bien que ces aspects soient effectivement traités par le RGS, ils ne sont que la partie immergée de l'iceberg. Sa « mise en place » est surtout l'occasion de cartographier le SI, de formaliser une politique de sécurité globale et pilotée, de pousser une approche flexible et adaptable au regard des moyens et des enjeux dans un contexte où la réactivité est nécessaire.

Dans ce contexte le RSSI privilégie une vision pragmatique à travers les besoins de sécurité des usagers. Le référentiel est l'occasion d'une vraie prise de conscience des équipes (IT et métiers) à la maîtrise des risques. Enfin le RGS est une opportunité permettant de responsabiliser les élus de la collectivité (via la mise en place de l'autorité d'homologation).

Les atouts et limites du RGS – Par Sébastien Herniotte

Le RGS est un texte de loi centré sur les échanges électroniques, mais ne traite pas du stockage des données. Le recours à des produits et prestataires qualifiés n'est pas imposé.

Afin de faciliter sa mise en application, il serait opportun de créer un guide thématique de mise en œuvre de l'homologation RGS.

L'homologation de sécurité est une approche par les risques permettant d'atteindre le juste niveau de sécurité. Favorisant le pragmatisme, le référentiel n'impose pas d'analyse de risques pour les projets de faible taille (par exemple les « petits » tmarioélé-services). Le RGS parait trop centré autour des échanges électroniques et ne traite que les mesures de sécurité statiques ne permettant pas de réagir aux nouvelles menaces des cyber-attaquants[3]. Le Référentiel n'est pas assez régulièrement mis à jour : de l'ordonnance de 2005 à aujourd'hui une seule version a été publiée officiellement. Enfin, le RGS ne précise pas la variabilité de la démarche, à savoir, une homologation simplifiée, standard ou complète.

La qualification des prestataires de services s'effectue via un schéma solide.[4] Il faudrait labelliser des sociétés de conseil pour l'accompagnement à la mise en œuvre du RGS.

---

[1] http://www.ssi.gouv.fr/fr/menu/actualites/publication-du-referentiel-d-exigences-applicable-aux-prestataires-d-audit-de.html

[2] Autorité Qualifiée de Sécurité des Systèmes d'Information

[3] https://www.clusif.fr/fr/production/ouvrages/pdf/CLUSIF-2013-Panorama-Cybercriminalite-annee-2012.pdf

[4] http://references.modernisation.gouv.fr/proc%C3%A9dure-de-r%C3%A9f%C3%A9rencement-0

En dernier lieu, en ce qui concerne les produits qualifiés, l'offre étant aujourd'hui trop restreinte sur le marché français, il serait pertinent de généraliser les exigences du RGS au niveau européen.

Le CLUSIF prépare une future conférence thématique traitant du RGS dans sa version 2.0.

Retrouvez les vidéos de cette conférence et les supports des interventions sur le web CLUSIF
http://www.clusif.fr/fr/infos/event/#conf131024.