ARKOON
NETWORK SECURITY

La conformité au RGS : un gage de sécurité pour les administrations

La sécurité informatique, désormais une exigence vitale, se positionne au cœur des schémas directeurs des grands donneurs d'ordres publics. De nombreuses initiatives, dont la création de l'ANSSI n'est pas la moindre, ont donc été menées par l'Etat afin de définir et mettre en place des référentiels et des bonnes pratiques visant à protéger les administrations d'actes de piratage. Ces pratiques tendent aussi à gagner ou à renforcer la confiance des usagers qui échangent avec l'administration par voie électronique.

C'est ainsi que le RGS est né. Créé par la DGME et l'ANSSI, le Référentiel Général de Sécurité (RGS) traite de l'ensemble des thématiques et des composantes de la sécurité des systèmes d'information et des échanges électroniques et en fixe les règles. L'application de ce texte est obligatoire pour les entités concernées – les autorités administratives – et le RGS peut être considéré comme un recueil de bonnes pratiques pour tous les autres organismes.

La mise en œuvre du RGS repose sur une démarche imposée, en trois volets :

- **Une analyse du risque**. Elle identifie les menaces portant sur le SI et leur impact sur l'activité de l'organisme ;
- **La définition des objectifs de sécurité et des mesures de sécurité** à mettre en œuvre pour réduire les risques identifiés ;
- **Une attestation formelle** que les exigences de sécurité sont bien déterminées et satisfaites, et que les risques résiduels sont maîtrisés et acceptés.

Cette démarche permet au RSSI (Responsable de la sécurité des systèmes d'information) de chaque administration de prendre les mesures nécessaires pour sécuriser au mieux son S.I. et sensibiliser ses collaborateurs aux bonnes pratiques à adopter en matière de sécurité informatique. Le respect du RGS assure également une prévoyance pour le RSSI ou l'AA (Autorité administrative) dont la responsabilité est clairement engagée dans la démarche sécurité du S.I. En effet, une analyse de risque incomplète ou des mesures de protection inadaptées peuvent être à l'origine d'un sinistre qui pourrait être personnellement préjudiciable au RSSI ou à l'AA. La définition précise d'un objectif de sécurité*, une mise en œuvre ad hoc et l'appui sur des fournisseurs de sécurité qualifiés instaurent autant de garanties pour assurer l'efficacité du dispositif de sécurité déployé.

En mai 2013, toutes les administrations devront s'être conformées au RGS, autrement dit avoir entrepris une démarche d'analyse, de réduction et d'acceptation du risque. Cette exigence répond de manière efficace et pragmatique aux enjeux et besoins légitimes de sécurité de l'administration qui doit montrer l'exemple en protégeant le « cyberespace public ». En effet, il est fondamental de gagner la confiance des administrés qui communiquent avec l'administration en garantissant l'intégrité et la confidentialité de leurs données personnelles.

Conformément au RGS, les administrations doivent également veiller à sélectionner des partenaires et fournisseurs qualifiés qui offrent des garanties en matière de continuité de service et d'intégrité des données qu'ils traitent. Les fournisseurs qualifiés présentent la garantie d'avoir investi fortement pour faire évoluer leurs offres et proposer des infrastructures de

Siège Social
T : +33 (0)4 72 53 01 01 • F : +33 (0)4 72 53 12 60 •
1, place Verrazzano • 69009 Lyon •
S.A au capital de 5 491 228€ RCS Lyon 428 173 975
www.arkoon.net

SkyRecon Systems
T : +33 (0)1 57 63 67 00 • F : +33 (0)1 57 63 67 37 •
An Arkoon comany • Immeuble le Pelissier
220, Avenue Pierre Brossolette • 92240 Malakoff
www.skyrecon.com

confiance, c'est-à-dire qualifiées par l'ANSSI comme répondant aux standards de sécurité exigés. On notera à ce propos que la plupart des administrations ont besoin de produits qualifiés au niveau standard (et rarement élémentaire) en raison de la sensibilité des données qu'elles manipulent**.

Se distinguer comme partenaire de confiance représente un investissement important pour les professionnels de l'IT, mené sur le long terme pour offrir des solutions actualisées, dotées de niveaux de sécurité garantis. A ce jour, peu de fournisseurs de solutions peuvent se prévaloir d'un tel engagement. Or, la qualification des solutions permet de garantir aux administrations un niveau de sécurité important, sur les points essentiels de leurs objectifs de sécurité, et conforme à l'état de l'art des attaques.

En imposant le RGS, les pouvoirs publics démontrent une nouvelle fois le rôle moteur de l'Etat dans la modernisation de sa relation avec les administrés. En ce sens, la France se positionne comme l'un des pays les plus en avance au niveau européen et contribue activement à mettre en place un dispositif performant qui lui permet de se protéger de menaces toujours plus complexes et pressantes.

Voir aussi
http://www.ssi.gouv.fr/fr/reglementation-ssi/referentiel-general-de-securite/

* Un objectif de sécurité fait partie intégrante de toute méthode de management de la sécurité.

L'analyse de risque permet de définir des objectifs de sécurité pour réduire ces risques, par exemple :
- Contrôler physiquement l'accès aux locaux
- Chiffrer les sources d'un logiciel sur un portable quand on intervient chez un client
- Authentifier les utilisateurs de manière forte
- Signer numériquement les ordres de transaction bancaire
- Etc.

Un objectif de sécurité est assuré par des mesures de sécurité qui peuvent être
- organisationnelles (par exemple, tout document papier confidentiel ne doit pas être mis à la poubelle, mais broyé)
- ou techniques (par exemple, des logiciels de chiffrement, des boîtiers de sécurité, etc.).

** Pour apprécier la robustesse des produits dans le cadre de la sécurisation de l'administration électronique, l'ANSSI procède à leur qualification, selon trois niveaux : élémentaire, standard et renforcé.
- Elémentaire : a pour objectif de vérifier que le produit est conforme à ses spécifications de sécurité, de coter ses mécanismes de façon théorique, de recenser les vulnérabilités connues de produits de sa catégorie et de soumettre le produit à des tests visant à contourner ses fonctions de sécurité.
- Standard : Le niveau est atteint si le produit permet de résister à un attaquant doté d'un potentiel d'attaque élémentaire au sens des Critères Communs. Il s'agit d'une procédure beaucoup plus contraignante, durant de 9 mois à 3 ans. Elle consiste à certifier le produit en EAL3, à faire passer en sus des tests d'intrusion de niveau EAL4 ainsi que d'autres composants d'assurance définis par l'ANSSI. Pour obtenir une telle qualification, un éditeur DOIT faire expertiser son code crypto par l'évaluateur, ce qui revient à lui fournir son code source.
- Renforcée : c'est le niveau le plus élevé, généralement réservé à des composants matériels. Il inclut notamment des tests de résistance de niveau EAL6.

Pour rappel, la CSPN (certification de sécurité de premier niveau) offre un premier niveau d'évaluation, en temps contraint, des fonctionnalités de sécurité proposés par des produits. Deux objectifs sont recherchés lors de l'évaluation :
- vérifier que le produit est conforme à sa spécification pour ce qui concerne sa sécurité ;
- déterminer l'efficacité des fonctionnalités de sécurité proposées par le produit.
La procédure dure entre 2 et 4 mois. La CSPN n'inclut pas de réel test d'intrusion.

Siège Social
T : +33 (0)4 72 53 01 01 • F : +33 (0)4 72 53 12 60 •
1, place Verrazzano • 69009 Lyon •
S.A au capital de 5 491 228€ RCS Lyon 428 173 975
www.arkoon.net

SkyRecon Systems
T : +33 (0)1 57 63 67 00 • F : +33 (0)1 57 63 67 37 •
An Arkoon comany • Immeuble le Pelissier
220, Avenue Pierre Brossolette • 92240 Malakoff
www.skyrecon.com