Externalisation et sécurité

Les entreprises et les administrations peuvent choisir de confier à un tiers tout ou partie d'une activité qui pourrait être réalisée en interne. Dans le domaine des systèmes d'information (SI), cette **externalisation** est appelée **infogérance**.

Ces prestations peuvent induire, en fonction du contexte dans lequel elles sont réalisées, des **risques pour le système d'information comme pour les données** (intégrité, disponibilité, confidentialité). On identifie trois grands domaines de risques (plus d'informations à l'intérieur) :

- La perte de maîtrise du système d'information ;
- Les interventions à distance ;
- L'hébergement mutualisé.

Pour autant, externalisation et sécurité des systèmes d'information ne doivent pas être opposées, et le recours à un prestataire est même souhaitable lorsque les compétences en interne sont absentes ou insuffisantes.

Parce qu'il est indispensable, dans toute opération d'externalisation, de **faire appel à des prestataires qui s'engagent sur la sécurité**, l'ANSSI propose un guide de l'externalisation qui vous aidera à maîtriser les aspects de sécurité dans les marchés d'infogérance.

Le guide propose une démarche pour **apprécier les risques** et fixer les exigences qu'appelle votre contexte, afin de **garantir la sécurité** de votre système d'information et des données qu'il traite. Il s'appuie pour cela sur le **plan d'assurance sécurité** et fournit des clauses types permettant d'obtenir du prestataire des engagements contractuels.

Rendez-vous sur le site de l'ANSSI
pour télécharger le guide :
http://www.ssi.gouv.fr/externalisation

Le cas du *Cloud Computing*

L'informatique « en nuage » (*Cloud Computing*), qualifiée parfois de « nébuleuse », est « *un mode de traitement des données d'un client, dont l'exploitation s'effectue par l'Internet, sous la forme de services fournis par un prestataire.* » C'est en outre « *une forme particulière de gérance de l'informatique, dans laquelle l'emplacement et le fonctionnement du nuage ne sont pas portés à la connaissance des clients.* »*

Les offres publiques ayant émergé ces dernières années proposent des services variés, accessibles via Internet, sur une infrastructure distribuée permettant d'assurer une grande disponibilité du service à un coût *a priori* réduit.

Mais de par leur nature, ces offres tendent aussi à **cumuler d'importants risques** inhérents à l'infogérance, en particulier :

- Risque pour la confidentialité des données ;
- Risque juridique à cause de l'incertitude sur la localisation des données (en particulier pour les données à caractère personnel, le patrimoine scientifique et technique) ;
- Risques liés à la perte de maîtrise du système d'information (forte dépendance au prestataire quant aux choix techniques, incapacité à déceler et gérer les incidents) ;
- Risque de captation de clientèle (irréversibilité).

Les contrats d'adhésion proposés dans le cadre des offres publiques ne couvrent généralement pas ces risques, et il est souvent impossible d'y introduire les garanties permettant de prendre en compte les exigences de sécurité et d'y répondre.

Pour toutes ces raisons, l'ANSSI recommande d'**étudier attentivement les conditions des offres**, de manière à apprécier les risques et la possibilité de mettre en œuvre un plan d'assurance sécurité approprié.

* Définition parue au Journal Officiel. Cette définition s'applique à l'informatique en nuage public, et ne concerne pas les nuages privés (dans l'entreprise) ou communautaires (partagés entre plusieurs entités identifiées).

Agence nationale de la sécurité des systèmes d'information
ANSSI – SGDSN – 51, boulevard de la Tour-Maubourg – 75700 PARIS 07 SP
Sites Internet : www.ssi.gouv.fr et www.securite-informatique.gouv.fr
Messagerie : communication [at] ssi.gouv.fr

→ Pour télécharger le guide de l'externalisation et découvrir le plan d'assurance sécurité, rendez-vous sur http://www.ssi.gouv.fr/externalisation

Le plan d'assurance sécurité (PAS)

Le guide de l'externalisation propose d'avoir recours à un plan d'assurance sécurité et fournit des clauses types à inclure dans le cahier des charges.

La fourniture d'un PAS doit être demandée dans l'appel d'offres. Rédigé par le prestataire, il décrit l'ensemble des dispositions spécifiques que celui-ci prendra pour **garantir le respect des exigences de sécurité** du donneur d'ordre.

Le PAS est un **document contractuel** : il constitue la réponse du futur prestataire aux exigences de sécurité définies dans le cahier des charges. L'exigence de fourniture d'un PAS se substitue à la clause générique de sécurité du prestataire.

Le PAS est un **cadre de réponse** : il offre une structure pour la réponse des soumissionnaires aux exigences de sécurité, ce qui permet de mieux évaluer la pertinence de la couverture des exigences. Il facilite ainsi la comparaison des différentes offres au regard des garanties proposées.

Grâce à une clause spécifique, le PAS peut être modifié lors de l'exécution du marché pour répondre à des évolutions du système, de son environnement ou du périmètre de l'opération. Cette souplesse garantit que les mesures prises par le prestataire seront toujours adaptées aux exigences de sécurité.

Agence Nationale de la Sécurité des Systèmes d'Information
Premier ministre
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Externalisation des systèmes d'information

Quels sont les risques de l'infogérance ?
Comment déterminer les exigences de sécurité ?
Quelles sont les clauses essentielles pour maîtriser les risques ?

UN GUIDE POUR MAÎTRISER LES RISQUES DE L'INFOGÉRANCE

Les risques de l'infogérance

Risque de perte de maîtrise du système d'information

Un certain nombre de facteurs peuvent être à l'origine d'une perte de maîtrise du système d'information :

- ✗ Sous-traitants non fiables, sous-traitance en cascade ;
- ✗ Localisation des données non maîtrisée ;
- ✗ Conséquences des choix techniques du prestataire (sécurité, interopérabilité).

Risques liés aux interventions à distance

Les dispositifs utilisés, souvent vulnérables, introduisent de nouveaux risques :

- ✗ l'intrusion sur le système d'information en exploitant une faiblesse du dispositif ou
- ✗ un abus de droits par un technicien

peuvent entraîner l'indisponibilité du système d'information ou des atteintes à la confidentialité et/ou à l'intégrité des données.

Risques liés à l'hébergement mutualisé

Même s'il n'est pas directement concerné, un service co-hébergé peut être affecté lorsqu'un autre service ou une des ressources mutualisées (réseau, matériel, logiciel) est victime d'un incident.

L'hébergement mutualisé est également susceptible de générer des obstacles supplémentaires pour répondre à un incident.

Prendre en compte la sécurité dans les marchés d'infogérance

Apprécier les risques et les traiter de façon adaptée
→ choix d'une stratégie de traitement des risques

Déterminer les objectifs de sécurité

Intégrer les exigences de sécurité dans le cahier des charges

Plan d'Assurance Sécurité

Choix du prestataire

Exemple : infogérance d'un site de commerce électronique – risques possibles :

Mon site pourrait subir les conséquences d'attaques ou incidents à répétition.

Si mon site venait à tomber en panne à l'approche des fêtes, mon bilan en serait sérieusement affecté.

Si ma base de données clients était compromise, l'image de marque de mon entreprise pourrait en pâtir.

Objectifs de sécurité possibles :

Le site ne doit pas être hébergé dans un environnement mutualisé.

Le site ne doit pas être indisponible.

Les configurations doivent être maintenues à jour.

Le site doit être protégé contres les intrusions de toute nature.

Exigences de sécurité :

Le système doit être hébergé sur des serveurs dédiés.

Le service doit être assuré avec un taux de disponibilité de 99,9%.

Un contact technique et un contact décisionnel sont mis à disposition du client ; ils doivent être joignables 24H/24 et 7j/7.

Le client doit pouvoir avoir accès aux journaux d'événements dans un délai de 24 heures.

Les correctifs de sécurité doivent être appliqués sur tous les composants logiciels dans un délai de 48 heures.

Des audits de sécurité incluant des tests d'intrusion seront réalisés par une société tierce. L'hébergeur appliquera les recommandations qui en découleront.

Les interventions à distance doivent garantir la confidentialité et l'intégrité des données. Les actions doivent être tracées.

À retenir...

Le principe

Chaque opération d'infogérance doit s'accompagner d'une étude préalable visant à **apprécier les risques**.

Chaque risque est traité selon une **stratégie** adaptée. Il en découle des **objectifs de sécurité.**

En vue d'atteindre ces objectifs, des **exigences de sécurité** sont intégrées au cahier des charges. Le prestataire répond à ces exigences dans un **Plan d'Assurance Sécurité** (voir au verso) apportant des garanties contractuelles.

Conditions essentielles de maîtrise des risques

- ✔ Procéder à une **analyse des risques** du système d'information.
- ✔ Étudier attentivement les **conditions des offres**, la possibilité de les adapter à des besoins spécifiques ainsi que les limites de responsabilité du prestataire.
- ✔ Imposer une **liste d'exigences précises** au prestataire, en particulier sur la réversibilité du contrat, la réalisation d'audits, la validation de certains choix techniques, la sauvegarde et la restitution des données dans un format ouvert normalisé ou encore le maintien à niveau de la sécurité dans le temps.