ROYAUME DU MAROC

ADMINISTRATION DE LA DÉFENSE NATIONALE

DIRECTION GÉNÉRALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

GUIDE RÉGISSANT LA SÉCURITÉ RELATIVE À L'EXTERNALISATION DES SI

INFORMATIONS

AVERTISSEMENT
Destiné à vous assister dans l'adoption d'une démarche cohérente et homogène pour la mise en conformité de la sécurité de vos systèmes d'information avec les règles de sécurité édictées par la Directive Nationale de la Sécurité des Systèmes d'information (DNSSI), ce guide élaboré par la DGSSI traite les bonnes pratiques relatives à l'externalisation des Systèmes d'Information. Il est destiné à évoluer avec les usages, mais aussi avec vos contributions et retours d'expérience. Les recommandations citées dans ce guide sont livrées en l'état et adaptées aux menaces au jour de leur publication. Au regard de la diversité des systèmes d'information, la DGSSI ne peut garantir que ces informations puissent être reprises sans adaptation sur les systèmes d'information cibles. Dans tous les cas, la pertinence de l'implémentation des éléments proposés par la DGSSI doit être soumise, au préalable, à la validation du Responsable de la Sécurité des Systèmes d'Information (RSSI) et de l'administrateur du système concerné.

PERSONNES AYANT CONTRIBUÉ À LA RÉDACTION DE CE DOCUMENT :

Rédigé par	Version	Date
DGSSI	1.0	12/12/2014

ÉVOLUTION DU DOCUMENT :

Version	Date	Nature des modifications
1.0	12/12/2014	Version initiale

PUBLIC CONCERNÉ PAR CE DOCUMENT :

Direction SI
RSSI
Maîtrise d'ouvrage

POUR TOUTE REMARQUE :

Contact	Email
DGSSI	contact@dgssi.gov.ma

Table des matières

1 Introduction

Le recours à l'externalisation dans le domaine des systèmes d'information est devenu une pratique courante qui présente un certain nombre d'avantages, mais aussi des risques en matière de sécurité des systèmes d'information qu'il convient d'évaluer. Ces risques peuvent être liés notamment à des spécifications contractuelles déficientes ou incomplètes.

Ce guide expose ces risques ainsi que les points clés à prendre en considération lors de l'externalisation du système d'information. En outre, ce guide a pour principaux objectifs de :

- Sensibiliser les décideurs aux risques en matière de sécurité des systèmes d'information liés à toute opération d'externalisation ;
- Fournir un ensemble de mesures préventives visant à atténuer les risques relatifs à une opération d'externalisation.

Il est à noter que les mesures énumérées tout au long de ce guide ne sont pas exhaustives. Il s'agit d'une base minimale qui doit être complétée par des mesures particulières prises par l'entité selon son contexte et ses besoins de sécurité.

2 Définitions

Pour une entité, l'externalisation du système d'information, dite infogérance, permet de confier, partiellement ou dans sa totalité, la gestion du système d'information à un prestataire dans le cadre d'un contrat, avec un niveau de services et une durée définis.
En fonction des besoins et des moyens de l'entité, cette externalisation peut se décliner en deux catégories : globale ou partielle. L'infogérance partielle regroupe également plusieurs types de services.

2.1 Infogérance globale

L'infogérance globale revient à confier l'intégralité de la gestion du système d'information à un prestataire qui prend en charge les fonctions de traitement, de développement, d'exploitation et de maintenance des applications et des équipements informatiques.

2.2 Infogérance partielle

L'infogérance partielle ne couvre qu'une partie du système d'information. On compte ainsi plusieurs types possibles, dont trois qui sont les plus importants :

- **Gestion des infrastructures**

Ce type d'infogérance s'axe autour de la fonction exploitation des systèmes d'information. La gestion des infrastructures permet d'externaliser l'hébergement ou l'exploitation des infrastructures informatiques, auprès d'un prestataire capable de gérer la complexité croissante de ces systèmes, de les rationaliser et de s'engager sur un haut niveau de satisfaction des utilisateurs.

Dans ce cas, il peut s'agir de la maintenance d'un parc informatique, de l'hébergement et/ou de l'administration de serveurs, de la supervision d'équipements réseau et de sécurité, de la gestion de baies de stockage ou de solutions de sauvegarde, etc.

- **Tierce Maintenance Applicative (TMA)**

Cela consiste donc pour une entité, à confier la gestion d'une application à un prestataire. Ce type d'infogérance gère ainsi tout ce qui se rapporte aux licences, à la gestion de cycle de vie, aux mises à jour des applications, etc. La tierce maintenance applicative couvre les activités de support fonctionnel aux utilisateurs, maintenance corrective, maintenance préventive, maintenance évolutive.

• **Le Business Process Outsourcing (BPO)**
Le prestataire héberge pour le compte de l'entité une application utilisée comme un service, accessible le plus souvent par le biais d'un navigateur web ou d'une application spécifique. Dans ce cas, l'entité n'est pas gestionnaire de l'application qu'il exploite pour traiter ses données et s'affranchit totalement des moyens pour la mettre en œuvre.

2.3 Cloud Computing

En pleine expansion, le cloud Computing représente une autre branche de l'infogérance. Ce dernier fournit des services ou des applications informatiques en ligne, accessibles partout, à tout moment, et de n'importe quel terminal (smartphone, PC de bureau, ordinateur portable et tablette). Précisément, le cloud Computing permet de partager, chez un fournisseur d'offres cloud, une infrastructure, une solution applicative ou encore une plateforme.
Différents modèles de Cloud coexistent :
• **Cloud privé/privatif :** ce cloud est interne à l'entité qui est propriétaire des infrastructures.
• **Cloud public :** ce cloud est externe à l'entité, géré par un prestataire externe propriétaire des infrastructures.
• **Cloud hybride :** Ici, il s'agit de la conjonction de deux ou plusieurs Cloud (public privé) amenés à « coopérer », à partager entre eux applications et données.

Il existe trois catégories majeures de services qui peuvent être offertes en cloud Computing :
• **Infrastructure as a Service (IaaS) :** consiste à fournir des ressources matérielles abstraites (serveurs, moyens de stockage, réseau…), typiquement des machines virtuelles, permettant d'installer à distance le système d'exploitation et les applications de son choix.
• **Platform as a Service (PaaS) :** fourniture de plateformes permettant le développement d'applications à partir d'interfaces de programmation (API) déployées et configurables à distance. Ce type de cloud concerne les environnements middleware, de développement, de test,…
• **Software as a Service (SaaS) :** fourniture d'applications directement utilisables à distance. Ce type de cloud concerne notamment les applications de type : outils collaboratifs, messagerie, informatique décisionnelle, ERP,…

Il existe d'autres services disponibles, notamment :
• **DasS (Desktop as a Service) :** est l'externalisation d'une machine virtuelle auprès d'un fournisseur de services. Généralement, le Desktop as a Service est proposé avec un abonnement payant.
• **STaaS (STorage as a Service) :** correspond au stockage de fichiers chez des prestataires, qui les hébergent pour le compte de l'entité. Des services grand public, tels que Dropbox, Google Drive, proposent ce type de stockage, le plus souvent à

des fins de sauvegarde ou de partage de fichiers.
• **CaaS (Communication as a Service) :** correspond à la fourniture de solutions de communication (autocommutateurs).
• **DTaaS (Data as a Service) :** correspond à la mise à disposition de données délocalisées quelque part sur le réseau. Ces données sont principalement consommées par des applications qui combinent du contenu ou du service provenant de plusieurs autres applications plus ou moins hétérogènes.

3 Cartographie des risques liés à l'externalisation des Systèmes d'Information

Parmi les risques de sécurité contre lesquels les entités doivent se protéger ou apporter une attention particulière en cas d'une opération d'externalisation de leur système d'information, on retrouve :

3.1 La perte de maîtrise du système d'information

• Difficulté d'intégration entre services disponibles en interne et ceux chez le prestataire ;
• Perte de gouvernance : l'entité cède nécessairement le contrôle au prestataire pouvant ainsi affecter la sécurité de son système d'information.

3.2 Risques liés à l'intervention à distance (télémaintenance)

L'infogérance implique souvent la mise en place de liaisons permettant d'intervenir à distance. En évitant le déplacement des techniciens, les interventions à distance permettent une réduction significative des coûts et des délais d'intervention.
Ci-dessous un certain nombre de vulnérabilités fréquemment liées aux dispositifs de télémaintenance :
• Liaison établie de façon permanente avec l'extérieur ;
• Présence de failles dans les interfaces d'accès ;
• Absence de traçabilité des actions ;
• Personnels responsables de ces dispositifs non conscients des problèmes de sécurité ou mal formés ;
• Interconnexion de systèmes sécurisés de confiance à des systèmes de niveau faible (internet par exemple) ;
• Mots de passe par défaut ou faibles.

3.3 Risques émanant de l'hébergement mutualisé

Les risques proviennent du fait que le service hébergé est plus ou moins étroitement lié à d'autres services, certains étant plus vulnérables que les autres. D'autre part, les attaques ciblant une des ressources mutualisées (réseau, logiciel, matériel) pourront avoir des conséquences sur l'ensemble des services co-hébergés. Du point de vue de la sécurité des systèmes d'information, les principaux risques

liés au co-hébergement et leurs répercussions sont les suivants :
• Perte de disponibilité : une attaque par déni de service provoque l'indisponibilité du serveur hébergeant la cible de l'attaque. Si plusieurs services sont hébergés sur le même serveur, les services qui n'étaient pas pris pour cible, de même que les équipements présents sur le chemin critique (pare-feu, routeurs, etc.) peuvent être indirectement victimes de l'attaque ;
• Les ressources reposent sur un matériel qui n'est pas contrôlé par le propriétaire de la ressource, mais par l'hébergeur. Il se peut qu'un problème matériel non contrôlé ait une répercussion à plus ou moins long terme sur la ressource confiée à l'hébergeur ;
• Perte d'intégrité : les vulnérabilités permettent souvent de s'introduire dans le système par exécution de code arbitraire causant ainsi l'installation d'une porte dérobée, la défiguration de site web, le vol d'informations, le rebond d'attaques, etc. Si un des services hébergés est pris pour cible d'une telle attaque, l'exécution de code peut toucher l'ensemble des services ;
• Perte de confidentialité : le partage du même environnement physique par des services peut conduire à des croisements d'information (contenu des fichiers clients de plusieurs sites dans la même base de données, ou le même sous répertoire, etc.) ;
• Isolation défaillante : les mécanismes de séparation des ressources (stockage, mémoire) peuvent être défaillants et l'intégrité ou la confidentialité des données compromises.

3.4 Non maitrise de la localisation des données

De par l'organisation des services du prestataire, les données qu'on lui confie peuvent se trouver dans n'importe lequel de ses centres de données, et de ce fait tomber sous la législation particulière du pays où se trouve ce centre.

Une localisation de données non maîtrisée peut comporter d'autres risques :
• Difficulté à exercer un droit de regard et de contrôle sur le personnel du prestataire ;
• Difficulté à effectuer un audit de sécurité de l'infrastructure sous-jacente.

3.5 L'accès non autorisé aux informations et aux locaux de l'entité

Suite à un acte d'ingénierie sociale, l'abus de droits d'un membre du personnel du centre de support du prestataire lors d'une intervention peut :
• Accéder à des données confidentielles ou télécharger massivement ces dernières ;
• Modifier des données sur le système d'information, éventuellement sans laisser de traces ;
• Causer des actes de sabotage.

3.6 Risques liés à la non réversibilité

La question de la réversibilité doit être une préoccupation permanente de l'entité. Quelles que soient les évolutions du système, l'entité doit être en mesure d'en reprendre l'exploitation à son compte, ou de la confier à un autre prestataire de son choix, et ce, à tout moment et sans difficulté particulière.

Le risque de perdre des données lors de la migration vers un autre prestataire ou une solution interne reste néanmoins présent.

3.7 Destruction ineffective des données, durée de conservation trop longue

Toutes les données concernant l'entité peuvent ne pas être complètement supprimées et ceci même après résiliation du contrat avec le prestataire.

3.8 Dépendance

• Lorsque un prestataire procède à une évolution dans sa structure (par exemple changement de logiciel), ceci peut avoir une répercussion indirecte sur un service hébergé (non compatibilité, erreurs, etc.) ;
• Lorsque l'entité souhaite procéder à une évolution, le prestataire peut ne pas être en mesure de suivre les besoins de l'entité sans pour autant affecter les services externalisés.

3.9 Faille dans la chaîne de sous-traitance

Un prestataire peut externaliser certaines tâches spécialisées de sa chaîne de production à des tiers. Dans une telle situation, le niveau de sécurité du prestataire dépendra du niveau de sécurité de chacun de ses sous-traitants.
Une sous-traitance en cascade peut rendre inefficaces les contraintes de sécurité exigées par l'entité.
Toute interruption dans la chaîne ou manque de coordination des responsabilités entre toutes les parties concernées peut conduire à une indisponibilité des services, voire une perte de confidentialité, d'intégrité et de disponibilité des données.

3.10 La cessation d'activité du prestataire

En cas de cessation de l'activité du prestataire, l'impact serait énorme sur l'entité. Ceci pourrait conduire à une perte ou détérioration de la performance de la prestation des propres services de l'entité.

3.11 L'indisponibilité du service du prestataire

L'indisponibilité du service du prestataire comprend l'indisponibilité du service en lui-même mais aussi l'indisponibilité des moyens d'accès au service (notamment les problèmes réseaux). L'impact de ce type de risque serait énorme pour l'entité.

3.12 Difficulté à tester et à mettre en œuvre un plan de continuité d'activité (PCA)

Pour garantir le maintien de la prestation, la mise en place des PCA s'avère nécessaire. La difficulté à définir, planifier et tester les PCA dans le cas d'une opération d'externalisation, réside dans la pluralité des acteurs vu que le sinistre pourrait affecter l'entité ou son prestataire.

4 Mesures préventives associées aux risques de l'externalisation des Systèmes d'Information

Dans le chapitre précédant, les principaux risques liés à l'externalisation ont été énumérés, mais il faut savoir qu'avec la mise en place de certaines bonnes pratiques, et en respectant quelques règles simples, il est possible de réduire de façon considérable ces risques et leurs impacts.

4.1 Conduire une analyse de risques

Pour toute entité, conduire une analyse de risques est essentiel pour pouvoir définir les mesures de sécurité appropriées à exiger du prestataire ou à mettre en interne.

La plupart des risques ont vocation à être traités par des dispositions contractuelles, pouvant inclure des mesures techniques et organisationnelles au niveau de l'entité et du prestataire.

Il est recommandé que l'entité évalue la pertinence de ces risques pour sa propre situation et étudie les mesures mises en place par elle-même et par le prestataire pour les réduire.

4.2 Éviter les offres d'externalisation gratuites

Si l'offre paraît attrayante, il ne faut pas perdre de vue le fait que la gratuité exonère le prestataire de sa responsabilité, celle-ci étant fixée à hauteur du prix de la prestation.

4.3 Maîtriser la chaine de sous-traitance

L'entité doit exiger d'être informée par le prestataire des sous-traitants auxquels il a recours et d'avoir la preuve que les engagements du prestataire vis-à-vis de l'entité sont bien répercutés à ces sous-traitants et qu'une sous-traitance en cascade ne rendra pas inefficaces ces engagements.

L'entité doit en outre, se réserver le droit de refuser tout sous-traitant ne présentant pas les garanties suffisantes pour exécuter les prestations conformément aux exigences de sécurité.

4.4 Localiser les données externalisées

Il convient de s'assurer que l'ensemble des lieux d'hébergement (site principal, site(s) de secours, de sauvegarde, etc.) répondent d'une part aux exigences de sécurité de l'entité, et d'autre part aux obligations légales et réglementaires, notamment en ce qui concerne la protection des données à caractère personnel. Cependant, l'hébergement de données sensibles de l'entité sur le territoire national est obligatoire.

L'entité doit exiger du prestataire que le contrat d'externalisation soit régit par la réglementation marocaine.

4.5 Exiger des solutions interopérables

L'entité doit imposer au prestataire que les applications utilisées dans le cadre de l'externalisation soient interopérables et compatibles minima avec les systèmes d'exploitation et les bases de données les plus courants.

4.6 Pouvoir assurer la réversibilité

La réversibilité a pour objet d'assurer la reprise partielle ou complète du système d'information par l'entité ou par un nouveau prestataire. Il est essentiel que l'entité prévoit les conditions de sa réalisation en précisant notamment :
• Le délai de mise en œuvre de la réversibilité ;
• Le format de transfert des fichiers et données (format « standard » du marché au jour de la réversibilité et/ou compatible avec le format utilisé par l'entité à cette date) ;
• Les conditions du transfert des logiciels/matériels dont serait titulaire le prestataire et qui seraient nécessaires à la continuité de l'exploitation par l'entité ;
• Les modalités d'assistance post-migration.

4.7 Contrôler les interventions à distance (télémaintenance)

Il est recommandé de demander au prestataire de recenser, de justifier et de décrire les dispositifs de télémaintenance qu'il envisage de mettre en œuvre sur le système de l'entité.

L'entité doit s'assurer que les dispositifs de télémaintenance satisfont au niveau de sécurité souhaité en exigeant du prestataire un descriptif des mesures techniques et organisationnelles proposées (la sécurité de la liaison, les procédures retenues pour déclencher une intervention, les droits d'accès, les mécanismes d'authentification, la traçabilité des actions…).

4.8 Privilégier l'hébergement dédié

L'hébergement sur une machine dédiée doit être privilégié. Il convient de préciser que, sauf demande explicite, une solution d'hébergement mutualisé sera prioritairement retenue par le prestataire. Si toutefois le choix d'un hébergement mutualisé est retenu, il convient de bien analyser les conséquences.

4.9 Assurer la sécurité des développements applicatifs

L'entité doit exiger du prestataire d'assurer la sécurité des développements applicatifs conformément à l'état de l'art dans chacune des technologies mises en œuvre, en respectant notamment les règles suivantes :
• Environnement applicatif maintenu en tenant compte des recommandations d'application de correctifs par les éditeurs ;
• Contrôle rigoureux des entrées utilisateurs ;
• Sécurisation des accès aux fonctions d'administration ;
• Principe du moindre privilège ;
• Mise en œuvre d'une gestion efficace des erreurs.

Pour la mise en œuvre de technologies web, l'entité peut préciser aux développeurs du prestataire qu'ils pourraient s'appuyer sur les recommandations de l'OWASP (Open Web Application Security Project).

4.10 Réaliser des audits de sécurité

L'entité doit pouvoir, à tout moment, contrôler que les exigences de sécurité sont respectées par le prestataire.

Le périmètre, la périodicité et les modalités du déroulement des audits de sécurité doivent être précisément déterminés selon des dispositions contractuelles bien définies.

4.11 Demander un plan d'assurance sécurité

Le Plan d'Assurance Sécurité (PAS) est un document contractuel, il décrit l'ensemble des dispositions spécifiques que le prestataire s'engage à mettre en œuvre pour garantir le respect des exigences de sécurité de l'entité.
Avant toute opération d'externalisation, il est recommandé que le prestataire fournisse un PAS à l'entité. Ce document définit en particulier l'organisation qui sera mise en place, la méthodologie à suivre pour gérer la sécurité du projet d'externalisation et les mesures techniques, organisationnelles et procédurales qui seront mises en œuvre dans les phases de transfert, d'exploitation et de réversibilité ou fin de contrat.

4.12 Respecter les règles de la Directive Nationale de la Sécurité des Systèmes d'Information (DNSSI)

En cas d'externalisation d'un système d'information, l'entité exige du prestataire de respecter les mesures et les recommandations figurant dans la Directive Nationale de la Sécurité des Systèmes d'Information.