10 recommandations pour maîtriser les risques dans le Cloud

Le Cesin (Club des Experts de la Sécurité de l'Information et du Numérique) en collaboration avec la CNIL, l'ANSSI et des juristes spécialisés vient de publier 10 recommandations pour maîtriser les risques dans le Cloud computing. Chez Verisafe, nous travaillons sur la sécurité du Cloud depuis plus de 6 ans et nous avons créé la méthodologie EFICAS (Evaluation Formelle et Indépendante du Cloud pour l'Adopter en toute Sécurité) destinée justement à maîtriser les risques dans le Cloud. Il nous est donc apparu intéressant d'analyser et de commenter les 10 recommandations du Cesin et de faire le lien éventuel avec notre méthodologie EFICAS.

Recommandation 1 : Estimez la valeur des données que vous comptez externaliser ainsi que leur attractivité en termes de cybercriminalité.

Comment estimer la valeur de nos données ? Quel sont les critères de valorisation ? Il s'agit ici de classifier les données que l'on souhaite externaliser. En pratique, cette classification dépendra du type de données utilisées. Pour des données de bureautique, elle peut être relativement simple comme par exemple une classification sur 5 niveaux basée sur deux critères : confidentialité et conformité.

Niveau	Désignation	Commentaires
1	Usage Interne	Accessible à l'ensemble du personnel
2	Réglementé CNIL (DCP)	Fait l'objet d'une règlementation en vigueur
3	Réglementé ASIP (DSCP)	Fait l'objet d'une règlementation en vigueur
4	Confidentiel entreprise	Droits d'accès approuvés par la hiérarchie
5	Stratégique entreprise	Acccès limité à une groupe de personnes

Mais pour d'autres projets Cloud, ce type de classification peut s'avérer totalement inadapté. Par exemple, dans un projet IoT où les objets connectés remontent des informations dans le Cloud, les critères de disponibilité et d'intégrité seront sans doute plus pertinents. Prenons l'exemple de sondes thermiques qui remontent des valeurs de température dans le Cloud. Ces données ne sont à priori pas confidentielles ni réglementées mais leur altération ou leur indisponibilité pendant une longue durée peut s'avérer critique. Dans la méthodologie EFICAS, nous préconisons de classifier toutes les données que l'on souhaite héberger dans le Cloud. Pour cela, nous avons développé une grille modulaire permettant de classifier facilement tout type de données qu'il s'agisse de données issues d'un SI classique,

d’un réseau industriel ou du monde de l’Internet des objets. Dans notre méthodologie, la classification des données n’est pas une étape strictement obligatoire mais elle permet, lorsqu’elle est réalisée, d’industrialiser le processus EFICAS pour un ensemble de projets.

Recommandation 2 : S’il s’agit de données sensibles voire stratégiques pour l’entreprise, faites valider par la DG le principe de leur externalisation

Sur le principe, cette recommandation tombe sous le bon sens mais en pratique, c’est quoi une donnée sensible ou une donnée stratégique ? Une DCP (Donnée à caractère personnel), c’est une donnée sensible ? La propriété intellectuelle dans le projet X c’est sensible ou stratégique ? Les données commerciales de l’agence Y, c’est sensible ? Au final, il sera difficile de savoir à quel moment et pour quel type de données, il convient d’obtenir une aval de la DG. Dans la méthodologie EFICAS, nous considérons qu’une validation par la DG est importante mais il ne s’agit en aucun cas de valider le principe de l’externalisation mais uniquement de valider les écarts entre risques tolérés par l’organisme et risques dans le Cloud après avoir epuiser tous les recours traditionnels de réduction des risques.

Concernant l’attractivité de vos données en termes de cybercriminalité, il s’agit effectivement d’un élément important qui permettra d’établir un niveau de menace sur vos données. Si vous stockez dans le Cloud des données sans aucun intérêt pour un concurrent, une agence de renseignement ou un cybercriminel, la faible attractivité de vos données entrainera un faible niveau de menace. Par contre, si vous stockez dans le Cloud des données de propriété intellectuelle stratégiques ou les numéros de carte bancaire de vos clients, l’attractivité sera radicalement différente et donc le niveau de menace bien plus élevé. Ce niveau de menace sera utile dans le processus d’analyse de risque lorsqu’il s’agira d’évaluer la probabilité d’occurrence des incidents de sécurité.

Recommandation 3 : Evaluez le niveau de protection de ces données en place avant externalisation.

C’est un élément également pris en compte dans la méthodologie EFICAS. En effet, le niveau de protection des données mis en œuvre dans l’organisme donne une première indication sur l’importance que l’entreprise accorde à ces données. Par exemple, le fait que les données soient stockées en clair (non chiffrées) et accessibles à un très grand nombre d’utilisateurs traduira sans doute une faible sensibilité de ces données en terme de confidentialité. Il s’agira alors de vérifier que dans le Cloud les données sont aussi bien, voire mieux protégées qu’en interne dans votre

entreprise.

Recommandation 4 : Adaptez vos exigences de sécurité dans le cahier des charges de votre appel d'offre en fonction du résultat du point 1.

Les exigences de sécurité peuvent effectivement être définies selon la valorisation des données issues de l'étape 1 mais également de l'étape 3. Il est en effet assez courant d'être beaucoup plus exigeants sur le niveau de sécurité d'une prestation externalisée que sur le même type de prestation réalisée en interne. Reste à savoir si ces exigences plus fortes vis-à-vis du prestataire sont justifiées. Dans la méthodologie EFICAS, plutôt que de partir sur des exigences de sécurité souvent difficiles à établir et à valoriser, nous démarrons le processus sur la base d'une cartographie des risques établis spécifiquement pour le Cloud computing. L'étape initiale consiste pour l'organisme à définir son niveau de tolérance pour chaque risque identifié.

Recommandation 5 : Effectuez une analyse de risque du projet en considérant les risques inhérents au cloud comme la localisation des données, les sujets de conformité et de maintien de la conformité, la ségrégation ou l'isolement des environnements et des données par rapport aux autres clients, la perte des données liée aux incidents fournisseur, l'usurpation d'identité démultipliée du fait d'une accessibilité des informations via le web, la malveillance ou erreur dans l'utilisation, etc. Sans oublier les risques plus directement liés à la production informatique : la réversibilité de la solution et la dépendance technologique au fournisseur, la perte de maîtrise du système d'information et enfin l'accessibilité et la disponibilité du service directement lié au lien Internet avec l'entreprise.

Une analyse de risque constitue bien évidemment une approche pertinente mais ici le Cesin n'identifie qu'une dizaine de risques et ne donne aucune indication pour les traiter. La méthodologie EFICAS établit une cartographie exhaustive des risques dans le Cloud (42 risques) et propose un arsenal complet de mesures spécifiquement adaptées aux problématiques dans le Cloud (CCM v3 de la CSA, ISO 27017 de l'ISO, contrat de cyber-assurance, …).

Après avoir sélectionné les risques pertinents dans le catalogue, Il faut ensuite être en mesure d'évaluer son propre niveau de tolérance aux risques. Dans un deuxième temps, il faut évaluer le niveau réel des risques dans le projet Cloud envisagé. La méthodologie EFICAS fournit aux entreprises tous les livrables nécessaires à la réalisation de ces deux étapes particulièrement délicates.

Recommandation 6 : Outre ces sujets, exigez un droit d'audit ou de test d'intrusion de la solution proposée.

« Exigez », c'est vite dit ! Demandez donc à Amazon, Google ou Microsoft un audit de sécurité sur leur infrastructure Cloud public. La réponse sera toujours négative. Vos exigences n'étant pas acceptées, que faire maintenant ? En pratique, la recommandation du Cesin n'est quasiment jamais applicable dans le cas d'un Cloud public. C'est la raison pour laquelle la méthodologie EFICAS propose une approche radicalement différente pour évaluer le niveau de sécurité du prestataire.

Recommandation 7 : A la réception des offres analysez les écarts entre les réponses et vos exigences.

Comme on vient de le voir à l'instant, on ne peut que rarement recourir à l'audit dans un Cloud public. Pour l'organisme client, il sera donc impossible de vérifier l'adéquation du niveau de sécurité du prestataire avec ses exigences. Comme indiqué lors de la recommandation (4), la méthodologie EFICAS permet d'établir une grille de tolérance aux risques plutôt qu'une liste d'exigences. Puisque l'audit n'est pas possible, EFICAS définit une liste d'évaluation des risques auquel l'organisme s'exposera dans le Cloud. Il suffira ensuite de contrôler les écarts entre risques tolérés par l'organisme et risque exposés dans le projet Cloud et de traiter les risques inacceptables avec les mesures spécifiquement adaptées au Cloud (CCM v3, ISO 27017, ISO 27018, assurance, …).

Recommandation 8 : Négociez, négociez.

Dans le Cloud et contrairement aux contrats d'infogérance classique les négociations avec le fournisseur sont assez limitées et parfois même inexistantes. On constate en effet aujourd'hui un déséquilibre de rapports de force entre les entreprises clientes et les fournisseurs. Ces derniers proposent le plus souvent des contrats standards non négociables. Pour bien comprendre cette difficulté, on peut citer l'expérience réelle d'une grande entreprise française du CAC 40 qui souhaitait négocier de nouvelles clauses de sécurité avec Google Inc. au lendemain des révélations d'Edward Snowden. Après de multiples tentatives y compris un rendez-vous avec la direction au siège social de Google France à Paris, le fournisseur américain a rejeté toutes les demandes du client et n'a en conséquence modifié aucune clause contractuelle. Face à Amazon, Google, Salesforce ou Microsoft, le rapport de force est souvent à l'avantage des fournisseurs américains même pour une grande entreprise cliente. Il va sans dire que les possibilités de négociation sont encore plus

hypothétiques pour une PME ou une collectivité territoriale.

Recommandation 9 : Faites valider votre contrat par un juriste. Si vous êtes une entreprise française, ce contrat doit être rédigé en français et en droit français.

Cette recommandation ne pose généralement pas de problème aux fournisseurs. Attention cependant à ne pas tomber dans l'excès comme l'ANSSI l'a fait dans son référentiel de qualification de prestataires de services sécurisés d'informatique en nuage. Si l'on suit les exigences de l'agence (localisation des données exclusivement sur le territoire français, support de premier niveau francophone localisé en France, contrat de droit français, tribunal compétent français), on risque fort de se retrouver devant une offre Cloud extrêmement limitée qui ne répondra pas aux attentes des métiers.

Recommandation 10 : Faites un audit ou un test d'intrusion avant démarrage du service (si cela est possible) et assurez-vous du maintien du niveau de sécurité de l'offre dans le temps.

On entre encore ici dans une difficulté particulière du Cloud, le contrôle de la sécurité. Comme le Cesin le sous entend en précisant « si cela est possible », les audits ne sont généralement pas admis sur une infrastructure Cloud public. Les fournisseurs acceptent plus souvent les tests d'intrusion (sur un périmètre précis) mais leur intérêt est extrêmement limité pour ne pas dire quasi nul. L'approche pragmatique de la méthodologie EFICAS permet de vérifier le niveau de sécurité du fournisseur même lorsqu'un audit n'est pas réalisable. La vérification est basée sur un questionnaire spécifique transmis au fournisseur. Elle est complétée par un contrôle approfondi des certificats de sécurité (ISO 27001, CSA STAR, ISAE3402, Privacy Shield, etc…).

D'autre part, la méthodologie EFICAS met l'accent sur le contrôle continu de la sécurité pendant toute la durée du contrat. Elle établit une liste de contrôles et une description détaillée de chaque paramètre de sécurité, ce qu'il faut mesurer et comment le mesurer. Parmi les paramètres de sécurité, on trouve par exemple la disponibilité du service, la réponse aux incidents, la gestion du cycle de vie des données, la conformité réglementaire, la gestion des vulnérabilités, le chiffrement des données, etc..