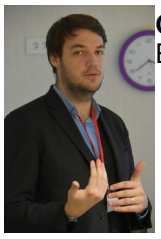
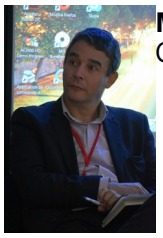
RENCONTRES PARLEMENTAIRES
COMPTE-RENDU ATELIER « CLOUD ET CYBERSÉCURITÉ »

Animateur

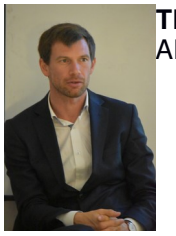


Quentin GAUMER, Club Cyber
École de Guerre Économique

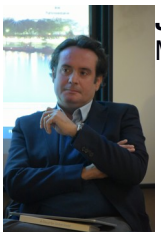
Participants



Mahmoud DENFER
CESIN



Thomas FILLAUD
ANSSI



Jean-Renaud ROY
Microsoft

David-Irving TAYER
ATIPIC Avocat

LE RÔLE DE L'ANSSI DANS LA SÉCURITÉ INFORMATIQUE RELATIVE AU CLOUD

Face aux enjeux bien précis relatifs au Cloud, l'ANSSI a été une force de recommandation. Elle a ainsi publié plusieurs référentiels à l'intention des entreprises y étant confrontées.

« L'ANSSI n'est « pas là pour créer de la loi ou du droit. »

De manière générale, selon les mots de Thomas Fillaud, l'ANSSI n'est « *pas là pour créer de la loi ou du droit* ». Le référentiel publié concernant le Cloud n'a ainsi pas force obligatoire. C'est au législateur qu'échoie cette responsabilité. Ces guides n'étant qu'indicatif et la Loi ne s'étant pas encore adaptée, rien n'empêcherait donc aujourd'hui une banque de stocker des données bancaires sur un Cloud quelconque.
L'ANSSI, ainsi cantonnée à la rédaction de guides indicatifs de sécurité, voit sa valeur ajoutée résider dans l'indépendance et l'impartialité totales de ces derniers. Il est bon de noter que les recommandations fonctionnent par pallier : la possession de données bancaires entraîne par exemple l'augmentation des règles de sécurité recommandées. Ce processus permet ainsi aux entreprises intéressées par la signature d'un contrat avec un prestataire Cloud d'effectuer une comparaison avec les conditions de celui-ci.

« Les référentiels et recommandations (de l'ANSSI) seraient trop axés sur les grandes entreprises et ne seraient pas applicables de manière réaliste aux petites et moyennes entreprises. »

Des critiques sont cependant opposées à cette démarche. Les référentiels et recommandations seraient « trop lourds », trop axés sur les grandes entreprises, et ne seraient pas applicables de manière réaliste aux petites et moyennes entreprises. Or ces dernières, en plus de représenter une partie importante du tissu économique français, sont tout autant soumises aux risques inhérents à l'utilisation du Cloud. La certification CSPN (Certification de Sécurité de Premier Niveau) délivrée par le Gouvernement constituerait à ce titre une alternative.

L'ANSSI se veut également une force de transparence, notamment en termes d'architecture technique : le client devrait selon elle être capable de savoir à un moment « T » où se trouvent physiquement ses données au sein du Cloud.

« Certains datacenters peuvent être jugés plus sûrs que d'autres. »

DE L'IMPORTANCE DE LA NÉGOCIATION CONTRACTUELLE

La signature d'un contrat avec un fournisseur Cloud n'a rien d'anodin et peut être porteuse de lourdes conséquences si elle est mal négociée.
Un des points critiques de cette négociation du contrat est la réversibilité des données. Pouvoir récupérer les données stockées chez un opérateur Cloud paraît être une évidence, cependant elle peut se révéler problématique en pratique. En cas de rupture du contrat, le client n'est parfois pas accompagné par son ancien opérateur, qui se contente de restituer les données en « brut ». La prévention d'un délai incompressible de négociation en cas de rupture, et ce dès la signature du contrat, est préférable. La coopération n'est en effet pas nécessairement optimale dans un contexte de crise ou d'affrontement entre les parties. Il faut également prévoir les dispositions à prendre en cas de dépassement de ce délai.

« Tous les fournisseurs n'imposent pas à leurs sous-traitants les mêmes engagements et obligations, ce qui peut générer une dilution des responsabilités, et donc de la sécurité des données stockées. »

La responsabilité des parties en cas de préjudice lié à une interruption de service (ex : messagerie hors-service sur une plage horaire durant laquelle d'importants appels d'offres avaient lieu) doit aussi être clairement définie lors de la signature. Un autre aspect à prendre en compte est la répartition des responsabilités au sein de la relation contractuelle. Lors de la signature avec un fournisseur Cloud, il y a bien entendu un transfert de compétences et de données, mais cela n'implique pas en soi de transfert de responsabilité. La responsabilité de chaque partie est précisément déterminée dans le contrat, qu'il est donc important de négocier.

Dans le prolongement de cette logique, les fournisseurs Cloud disposant eux-mêmes de sous-traitants, demander leur liste (et les mises à jour de celle-ci) est nécessaire. Cela n'est toutefois pas toujours simple, en fonction du pouvoir de marché ou de la nationalité de l'interlocuteur. Tous les fournisseurs n'imposent pas à leurs sous-traitants les mêmes engagements et obligations, ce qui peut générer une dilution des responsabilités, et donc de la sécurité des données stockées.

« La souveraineté du Cloud est donc une problématique de sécurité réelle, que l'État [doit] prendre au sérieux. »

De même, un contrat avec un fournisseur Cloud est une souscription. Les données appartiennent au client, mais pas l'environnement dans lequel elles sont hébergées. À titre d'exemple, l'offre Microsoft propose un environnement contenant plusieurs services. Le contrat détermine quels services sont utilisés, mais ceux-ci ne sont pas protégés de la même façon : la messagerie de Microsoft est ainsi basée en Europe, mais la vidéo l'est aux USA. De même pour d'autres services. Pour chacun de ces services, il est donc bon de savoir dans un contrat quelles données sont hébergeables en Europe, et lesquelles le sont aux États-Unis.
L'inertie géographique des *datacenters* peut entre autres être attribuée à l'âge des infrastructures, et à la législation.

LA QUESTION DE LA SOUVERAINETÉ DU CLOUD

Au fil du développement du Cloud se pose en parallèle des questions de la sécurité informatique celle de la souveraineté du Cloud. À titre d'exemple, 85% des entreprises du CAC40 se reposent sur Microsoft pour leurs besoins en Cloud. Une partie de leurs données, en fonction des services employés, sont donc hébergées sur le sol américain. Cela peut sembler anodin. Le cas de l'Allemagne est à cet effet intéressant : le pays a en effet pris une décision forte et mis en place des infrastructures et services nationaux, assurant à ses utilisateurs de Cloud allemands que leurs données ne seront pas accessibles à des forces étrangères. La souveraineté du Cloud est donc une problématique de sécurité réelle, que l'État allemand a prise au sérieux.
La question de la souveraineté est cependant un « non-sujet » aux yeux de l'ANSSI, qui refuse de raisonner en ces termes. Elle met ainsi en avant que l'Allemagne, ayant fait le choix d'un Cloud national et plus sécurisé, possède en conséquence un coût 35% plus élevé que le marché. Elle reconnaît cependant que « *la clientèle exigeante est celle qui fait avancer le marché de la sécurité informatique* ». Son indépendance vis-à-vis du Ministère de la Défense peut expliquer sa neutralité en la matière.
Il demeure que certains *datacenters* peuvent être jugés plus sûrs que d'autres. Ceux situés en Chine imposent ainsi aux opérateurs étrangers de mettre en place des infrastructures spécifiques, opérées uniquement par des citoyens chinois. L'hébergement dans de telles conditions a été déconseillée par les animateurs de l'atelier.

CE QU'IL FAUT RETENIR

- L'ANSSI n'est « pas là pour créer de la loi ou du droit.
- Les référentiels et recommandations (de l'ANSSI) sont trop axés sur les grandes entreprises et ne semblent pas applicables de manière réaliste aux petites et moyennes entreprises.
- Certains datacenters peuvent être jugés plus sûrs que d'autres.
- Tous les fournisseurs n'imposent pas à leurs sous-traitants les mêmes engagements et obligations, ce qui peut générer une dilution des responsabilités, et donc de la sécurité des données stockées.
- La souveraineté du Cloud est donc une problématique de sécurité réelle, que l'État [doit] prendre au sérieux.

L'utilisation de tout ou partie de ce compte-rendu doit s'accompagner d'une référence ©CyberCercle