Can we trust a Cloud provider with our most critical corporate assets ?

*By Dario ROSSA, Associate partner at Spike Reply**

Without a doubt, the Cloud is expanding at the speed of light. This morning I googled for "Cloud Security" and received 57 Million hits, a few hours later and it was already over 69 Million hits. Together with this incredible expansion, threats and cyber security risks are growing at the same speed. Moving your corporate applications and data onto the Cloud is a bit like leaving your child at kindergarten for the first time. It is scary to hand over corporate strategic information into someone else's control. Leadership teams, executives, security officers, information risk officers and the vast majority of stakeholders have the same question: Is the Cloud secure? Can we trust a Cloud provider with our most critical corporate assets? The short answer, to quote Obama is: "Yes, we can". However, the true answer is somewhat more nuanced.

Multi-tenancy

Multi-tenancy is more than just a buzz word, it is a necessity in order for cloud providers to operate as a profitable business. It is part of the strategic economies of scale of the cloud providers business. The bottom line is that sharing applications, operating systems, and data stores across multiple corporate clients generates cost savings for corporations. Of course, this also supports the business model and the economics of a Cloud provider.

Benefits include cost savings due to shared hardware and software licenses, efficient release management, and maintenance. Corporations can focus on the business part of their information technology strategy and not on the operational aspects. But what about our corporate data, which is being stored together with other clients' data?

Service Level Agreements (SLA) and Contracts

I am not a big fan of using analogies, but engaging with a cloud provider is almost like getting married. Having a long engagement period allows you to get to know your partner, with any perceived annoying behaviours that they may have and having a good contractual agreement in place will save you a lot of headaches when the relationship ends. This sounds horrible, but you need to be prepared for the worst. A risk-based approach is advisable and a risk-based approach is advisable when engaging with a cloud provider.

Often I hear the remark that corporations have no bargaining power with cloud providers. "Here are our terms and conditions, take it or leave it". This is a questionable approach to customer centricity, but it does happen. What can you do? Firstly, one could play the game of "We get these terms and conditions with supplier X, however we prefer your quality of services and would like to have the same conditions". Secondly, it does not hurt to position your cloud outsourcing project as being the largest and most strategic outsourcing project of your corporation. Do not be shy in your ambition! Let them know the importance and size of the project. Even if you start small, size does matter for a cloud provider. Make it appear bigger than it is.

Try to negotiate a contract with SLA that serve and support your business model, not theirs. It is important that cloud providers operate at your level of security requirements. It is your data, not theirs. You remain responsible and accountable over your data. Include penalties for non-compliance, but put the right metrics in place to support the proof required to achieve the required level of services and operations. Measuring brings knowledge. Make sure to include a notification obligation in case of a data breach or major security incident. Make sure you get insight into their annual audit reports, the results of their business continuity planning and disaster recovery tests. Include necessary exit conditions as it is better to be prepared in case the contract is terminated. Be aware of cascaded outsourcing.

Most of the cloud providers are using suppliers for their services as well. Make sure that there is complete transparency on all cascading dependencies. Make sure that you have appropriate, secure communication channels in place in case the cloud provider requires you as a client to enter the secret of the encryption key in the event of preventive maintenance or an unplanned restart.

Last but not least, agree on how to get the data back, both in the type of media and format, have an agreed timescale for receiving data, and have the assurance that all data will be deleted after the termination of the contract, including the requirement to provide the forensic proof-of-deletion.

Owning the secret of your encrypted data

Most cloud providers have encryption on the data storage in place, where this has been requested by the client. The problem is that most cloud providers have one common encryption key for the data of all their clients. Key management can become a hassle for most cloud providers. It is not only difficult to manage, but also it inhibits the performance of the cloud platform. The arguments of having a layered defense with multiple Demilitarised Zone (DMZ) will not block or mitigate all threats. Having encrypted communication channels is a mandatory requirement, but more important is your ownership of the secret of the encryption key. Make sure you own the secret of your encrypted data.

Additionally, you want to have an assurance that there is traceability of the complete life cycle of your encryption key. A Hardware Security Module (HSM) serve the purpose, however most cloud providers have not invested in the necessary key management infrastructure. Some cloud providers load the key into memory at startup, split into 2 parts and each part is owned by a key employee. Still, it requires the client to enter their key into memory at startup as well. Make sure that this procedure is clear for all stakeholders.

Backups and Data Retention

What happens if you terminate the contract with the cloud provider? Do you have the forensic proof that all data will be deleted from the cloud platform? Ask yourself, what would happen if one of your clients asked you to remove all records that your corporation is holding in the cloud. Could your cloud provider delete your individual client data? This is often a problem in a multi-tenancy cloud provider. Recently, the data retention EU Directive has been invalidated by the European court of justice, for a number reasons(1).

Still, I would recommend to keep the data retention period to the old stated requirements of the invalidated EU-directive and retain the data for a period of a minimum of 6 months up to a maximum of 2 years. Get the formal assurance of your cloud provider that it is handled with the same level of security controls as live data.

Regulatory Requirements

Consider whether your corporation is operating in a regulated market and therefore subject to regulatory requirements and obligations, making sure that processes are in place to notify the regulator on all activities related to moving applications and data into the cloud. Get the necessary exemptions and approvals from the regulator, as this will save you a lot of headaches in case of an audit or investigation. Do not forget that regulations are there to help you and to force you to follow best practices, they are here to protect you against cyber risks. It is a flawed approach for you to comply with regulations in order to just tick the box because it is an obligation, instead of getting the real security value out of regulatory requirements.

Personal Identifiable Information (PII)

The Safe Harbor Framework law is a good thing. However, it does not protect you against the US government accessing your data in case of a terrorist act or due to an event that could pose a danger to US national security. As we know, this interpretation of a possible event can be very elastic and as such there is no guarantee that the US government will not access your corporate data and PII. As a data controller, you need to know where your PII is stored, who has access to it and have full traceability on who has consulted the PPI at all time.

If you operate in a regulated market, some country-specific regulators require you to keep PPI stored within the EU-zone. Make sure this is the case with your cloud provider and notify the regulator in case you deviate from local or European regulatory requirements. Get a formal exemption to store the PII with the cloud provider. As some cloud providers can move data around without notifying their clients to optimise their operations, this point is relevant for many customers.

Conclusions

Moving your strategic corporate applications and data into the cloud is a critical and strategic choice. It is one of these decisions that require the attention and full support of the executive leadership team. Cloud providers are secure, but take a risk-based approach to moving your corporate application and data into the cloud. Assure that you are in control at all times over your applications and data.

In summary, here are some guidelines to further increase the assurance of having a secure cloud:
- Have a watertight contract in place with Service Level Agreements that serve your operations.
- Be aware of cascading outsourcing from a regulatory point of view.
- Make sure that you own the secret of the encryption keys used.
- Request notification obligation from your cloud provider in case of a data breach or security incident.
- Have insights in the regular vulnerability and penetration testing reports.
- Make sure annual business continuity and disaster recovery tests are executed during an entire day of life operations.
- Have complete traceability on the life cycle of your encryption keys.
-Select a cloud provider that allows your infrastructure to be cloud-agnostic.
- Negotiate and position your corporation as the next big thing. Size does matter.

Cloud Security, It matters how you establish it.

1) http://www.loc.gov/law/help/eu-data-retention-directive/eu.php

** Dario Rossa, Associate partner at Spike Reply, leads the cyber security practice for Benelux & France. Dario graduated from the TRIUM MBA program at the New York Stern School of Business, London School of Economics and HEC Paris. Dario also teaches Strategic Management (MIBEM) and Information Security Risk Management (Business Engineering) as a guest-professor at KU Leuven, Faculty of Economics. Dario can be reached at d.rossa@reply.eu*

FAIA : cette fois-ci, c'est parti !

Si FAIA(1), ce fichier électronique structuré pouvant être exigé par l'administration de l'Enregistrement, marquait le début d'une nouvelle ère pour les contrôles TVA au Luxembourg, l'obligation était jusque récemment en phase test et confinée à quelques entreprises pilotes. Depuis le début de l'année, les demandes se sont multipliées et ceci marque les débuts officiels des contrôles sur base de fichiers FAIA.

Les sociétés concernées doivent être capable d'extraire de leurs systèmes informatiques et de rassembler dans un seul fichier au format et à la structure définis, toutes leurs écritures comptables et une somme de données commerciales et financières existantes sous forme électronique.

Il n'existe encore que peu de systèmes informatiques permettant l'extraction des données sous le format requis. Et même les éditeurs de logiciels qui se sont équipés de modules adéquats peinent à fournir des fichiers acceptables pour l'administration.

Le premier défi est donc d'être capable de construire un fichier dont la structure et le contenu répondent aux normes FAIA. Un autre est de le rendre lisible aux financiers et aux fiscalistes avant qu'il ne soit soumis au contrôle de l'administration.

Le FAIA est un fichier XML, qui ne permet que très difficilement d'en visualiser le contenu et vérifier les données qui y sont incluses. Dès lors, comment construire un langage commun à l'ingénieur informatique au fiscaliste en passant par le CFO? Pour faire lumière sur les derniers développements en la matière, PwC Luxembourg a rassemblé plus de 80 professionnels le jeudi 25 juin.

Le FAIA représente une vraie avancée pour l'administration qui passe encore à un autre stade d'automatisation. Le logiciel qui lira ces fichiers devrait permettre de sélectionner certains points à vérifier en priorité par les inspecteurs du bureau d'imposition, et donc cibler au mieux les zones à risque au sein de sociétés pouvant traiter des milliers voire des millions d'opérations d'achats et de ventes et de paiements au cours d'une année.

Pour ces sociétés, par contre, l'investissement requis pour construire ce fichier est significatif. Les participants présents à la conférence de PwC Luxembourg ont confirmé que ces projets s'étendent sur des durées de plusieurs mois et monopolisent des ressources humaines internes et externes.

«Le nerf de la guerre pour les entreprises est de débloquer le budget et le temps nécessaire à ce projet, alors qu'elles sont encore souvent prises au dépourvu et se voient imposer des délais par l'administration. Il faut rappeler que la loi prévoit maintenant des contraintes pouvant aller jusqu'à 1000 euros par jour de retard dans la fourniture d'un fichier valide. Il leur faut gérer ensuite en urgence la difficulté d'inventorier, comprendre et rassembler toutes les données obligatoires, et elles sont nombreuses, dans un fichier unique et lisible par toutes les parties prenantes au sein de l'organisation», indique Frédéric Wersand, associé chez PwC Luxembourg. PwC Luxembourg a par ailleurs développé et présenté un outil permettant de lire les fichiers FAIA, visualiser le contenu et évaluer les données et leur cohérence. «Nous avons mis sur pied un outil de test qui s'assure que le format et la structure sont bons, mais aussi qui vérifie les données et traque les éventuelles erreurs avant envoi à l'administration», conclut Frédéric Wersand.

1) Fichier d'Audit Informatisé de l'Administration de l'enregistrement et des domaines

Le « mobile shopping » moins populaire au Luxembourg

Selon la dernière étude d'ING International Survey sur le mobile, il apparaît que moins de la moitié des résidents luxembourgeois (49%) ont indiqué avoir effectué un achat via mobile (smartphone ou tablette) ces douze derniers mois, contre 58% pour la moyenne européenne. La Turquie (84%), la Pologne (64%) et la Roumanie (62%) affichent le plus grand nombre de «mobile shoppers» tandis que la Belgique (37%), les Pays-Bas (42%) et la France (42%) sont en queue de peloton.

Par ailleurs, on constate que les vêtements et l'électronique sont les types de produits les plus fréquemment achetés via mobile. Entre les différents pays européens, on constate des nuances néanmoins: l'électronique caracole en tête en Turquie (47%), Italie (40%), en Roumanie (40%), en Espagne (33%), en République tchèque (26%) ou au Luxembourg (25%). Entre les sexes, on note également des différences partout en Europe: les hommes achètent davantage des gadgets électroniques tandis que les femmes achètent plus généralement des vêtements.

L'étude révèle aussi que mobile shopping va de pair avec mobile banking: près de 4/5èmes (79%) des utilisateurs européens du mobile banking ont fait un achat online via leur dispositif mobile, contre 34% pour ceux qui ne sont pas adeptes du mobile banking. Le Grand-Duché affiche des pourcentages assez proches de la moyenne européenne, avec respectivement 75% et 31%.

Parmi les catégories les plus susceptibles de faire leurs achats via mobile, on constate que les hommes devancent les femmes (61% contre 54% ; chiffres au niveau européen). Enfin, si l'on se penche sur l'utilisation par tranche d'âge, on constate que les jeunes adultes (25-34 ans) sont deux fois plus nombreux (74%) que les plus de 55 ans (37%) à faire du «mobile shopping».

Plus de détails sur eZonomics.com: http://www.ezonomics.com/ing_international_survey/mobile_banking_2015