Charlie Hebdo : Le FBI en 45mn chrono

Dans le cadre de l'affaire Charlie Hebdo, le directeur juridique de Microsoft, Brad Smith a révélé que Microsoft avait reçu une requête du FBI pour accéder au contenu des emails des frères Kouachi. Microsoft aurait mis 45 minutes pour analyser la validité de la requête, la juger légitime, rechercher les informations requises et les transmettre aux autorités américaines. Cependant, Brad Smith ne précise pas si les données étaient situées aux Etats-Unis ou en Europe et si une NSL (lettre de sécurité nationale utilisée dans le cadre de l'USA PATRIOT Act.) avait été utilisée par le FBI. Pour rappel, dans le cadre d'une enquête de trafic de drogue, Microsoft s'est opposé à une requête du FBI portant sur des emails stockés en Irlande, argumentant l'opposition du droit Européen (Directive 95/46 CE) et le fait que la justice irlandaise n'avait pas expressément donné son accord. Hélas, la juge fédérale Loretta Preska a décidé le 31 juillet 2014 de réfuter les arguments de Microsoft et ordonné le rapatriement des données stockées en Irlande vers les Etats-Unis. Microsoft a refusé de s'exécuter et a fait appel alors même que la juge Loretta Preska avait convenu que son jugement ne pouvait faire l'objet d'aucun appel et que Microsoft avait le devoir de s'exécuter. Affaire à suivre…

Autres ressources :

- Attentat à Charlie Hebdo : Microsoft n'a mis que 45 minutes à fournir des e-mails au FBI
- Attaque de Charlie Hebdo : Microsoft a livré des données au FBI
- Microsoft handed FBI data on Charlie Hebdo probe in 45 minutes
- Microsoft Gave Data on Charlie Hebdo Probe to FBI in 45 Minutes

---

Cloudwatt, c'est déjà fini ?

Face aux difficultés rencontrées, la totalité des titres de Cloudwatt devaient être rachetés par Orange. Cette annonce, bien que pas vraiment surprenante sur le fond, a fait l'objet d'un communiqué de Presse publié le 12 janvier 2015 dans lequel on peut lire :

« Depuis sa création en septembre 2012, Cloudwatt a bâti un projet industriel pérenne au profit du développement du cloud souverain en France. »

La société Cloudwatt lachée par l'état et rachetée par Orange moins de 3 ans après sa création, peut-on appeler cela un projet industriel pérenne ?

« Ces solutions d'avenir, qui s'inscrivent dans les évolutions du marché, ont déjà suscité l'intérêt de partenaires et clients de Cloudwatt. »
Commençons donc par juger la qualité des partenaires commerciaux et le nombre des clients puisque nous savons aujourd'hui que le CA de Cloudwatt ne devrait pas dépasser les 2 M€ en 2014. Pour information, en 2012, Cloudwatt annonçait une prévision de chiffre d'affaires annuel de 500 M€ en 2017.

« Thales a permis à Cloudwatt de mettre en place une plateforme cloud sécurisée. »
Il n'est pas question ici de remettre en cause les compétences de Thalès en matière de sécurité mais quels sont les arguments de Cloudwatt en matière de sécurité ? Voici les seules informations sur le sujet annoncées sur le site de Cloudwatt :
« Datacenter de production basé en Normandie, à Val de Rueil, équivalent tiers IV (taux de disponibilité : 99,95%) opéré par Orange »
Information surprenante quand on sait que pour obtenir une classification Tier IV de l'Uptime Institute (http://www.uptimeinstitute.org) le datacenter doit disposer d'un taux de disponibilité d'au minimum 99,995%. Il s'agit très certainement d'une coquille sur le site Web de Cloudwatt car une disponibilité de 99,95% ne permettrait même pas d'obtenir une certification Tier I. Mais quand il n'y a qu'un seul chiffre sur la sécurité des services et que celui ci est inexact, ça ne donne pas vraiment confiance. Pour information, il n'y a en France que 3 Datacenters officiellement certifiés par l'Uptime Institute. Deux sont en Tier III (Online SAS & Gemalto) et un seul en Tier IV (Crédit Agricole). Précisons pour finir que de nombreux fournisseurs Cloud annoncent des Datacenters certifiés Tier III+ et que cette certification n'existe tout simplement pas !
« 3 niveaux de sécurité pour accéder aux équipements hébergés dont un contrôle biométrique. »
Le contrôle d'accès physique c'est bien mais QUID des accès logiques, de la gestion des vulnérabilités, de la réponse à incident, de l'habilitation du personnel, etc… ? Dans ce contexte, tout client potentiel est en droit de se poser quelques questions comme par exemple :
Où est le livre blanc de la sécurité Cloudwatt qui explique clairement les mesures de sécurité mises en œuvre par Cloudwatt ?
Où sont les certificats de sécurité (ISO 27001 en particulier) délivrés par un tiers indépendant ?
Où sont les réponses au questionnaire (CAIQ) proprosé par la Cloud Security Alliance pour évaluer la sécurité des fournisseurs ?
Comment fait-on un PCA/PRA avec un seul Datacenter ?
Rien de tout ça chez Cloudwatt, pour qui la sécurité se résume en une phrase : « Un (unique ?) Datacenter situé en France ». Quand on sait que la sécurité reste le principal frein d'adoption au Cloud, on se demande pourquoi aucune information transparente et indépendante ne soit fournie par la société sur ce sujet.

Terminons enfin par une dernière citation du communiqué de presse d'Orange :
« L'Etat, initiateur du projet, aura rempli son rôle en contribuant à lancer une offre de cloud public capable de rivaliser avec les meilleurs tout en garantissant une souveraineté des données. »
Selon Orange, actionnaire principal de Cloudwatt avec 44,4% du capital, l'état aurait donc rempli son rôle en finançant (à hauteur de 75 millions d'euros) deux concurrents (Clouwwat et Numergy). Tout contribuable français est en droit de se demander si le lancement de deux fournisseurs en concurrence frontale soit une stratégie pertinente ? D'autre part, comment un investissement global de l'état de 150 millions d'euros peut-il permettre de rivaliser avec les leaders du marché quand on sait, selon des chiffres révélés par le Gartner, qu'Amazon, Microsoft et Google ont investi respectivement 12, 18 et 20,9 milliards de dollars dans leurs infrastructures de cloud entre 2005 et 2013 ?

Autres ressources :

- Les actionnaires de Cloudwatt engagent des discussions pour étudier la reprise de 100% de son capital par Orange
- Retour vers le futur – Cloudwatt, le souverain descend de son nuage…
- Reprise de Cloudwatt par Orange : un bien ou un mal ?
- Orange va reprendre 100% du capital de Cloudwatt
- Le Cloud souverain français patine : Cloudwatt devrait disparaître dans Orange

---

Key Vault, le HSM enfin disponible dans Azure

Bien plus tardivement que son principal concurrent Amazon avec son offre CloudHSM, Microsoft annonce enfin Key Vault, une solution HSM pour son cloud Azure. Key Vault permet une amélioration sensible de la sécurité des données par le stockage des secrets cryptographiques et des données sensibles dans un module de sécurité matériel (HSM) certifié FIPS 140-2 niveau 2 et Critères Communs EAL4 +.
Rappelons qu'un HSM renforce considérablement la sécurité des opérations cryptographiques asymétriques car la génération des bi-clés a lieu à l'intérieur du dispositif. Avec un HSM, la clé privée n'est jamais directement accessible aux administrateurs ou aux applications. Les opérations asymétriques devant invoquer la clé privée se déroulent donc exclusivement à l'intérieur du boitier HSM. Ainsi, ni un administrateur malveillant, ni même une faille critique comme heartbleed ne

peuvent permettre la compromission de la clé privée car elle ne se trouve jamais dans la mémoire utilisée par le système ou les applications.

Autres ressources :

- Avec Key Vault, Microsoft dote Azure d'un coffre pour clés de cryptage
- Microsoft Azure : Docker et chiffrement au menu 2015
- Key Vault – Windows Azure – Microsoft
- What is Azure Key Vault ?
- Azure Key Vault – Making the cloud safer

Arrêt du Cloud pendant 48H chez Verizon

Verizon vient d'annoncer que son cloud serait arrêté pour des raisons de maintenance pendant 48 heures. L'interruption débutera le samedi 10 janvier 2015 à partir de 13 heures (Eastern Time Zone), soit 7 heures du matin en France.

Il serait intéressant d'analyser ce que prévoit le contrat Verizon sur ce sujet. Une clause indiquant un arrêt exceptionnel de 48 heures pour des opérations de maintenance a pu être insérée dans le contrat et dans ce cas, aucune contestation possible. La jurisprudence en France est très claire sur ce sujet comme l'atteste l'affaire suivante :
Une société française avait subit une importante défaillance de son service de courrier électronique opéré dans le Cloud. Le service de messagerie ayant été rétabli au bout de 5 jours, la société cliente avait alors décidé de résilier le contrat aux torts du prestataire. Mais, la société cliente sera condamnée par le Tribunal de commerce de Paris le 12 juillet 2011. Le tribunal rappelle que l'entreprise est tenue par les termes du contrat qu'elle a souscrit. Elle devra alors payer les frais de justice du fournisseur ainsi que le montant des trimestres de son abonnement restant à courir. En effet, le contrat stipulait noir sur blanc un délai d'interruption du service admissible de 30 jours maximum.

Dans le cas de Verizon, si une telle durée d'interruption n'était pas prévue, Il faut regarder ce que prévoit le contrat Verizon en matière de pénalités ou d'indemnités. Attention cependant à ne pas confondre pénalités et idemnités qui sont deux choses bien différentes. Les pénalités viennent sanctionner le client ou le prestataire lorsqu'il est à l'origine du non-respect du SLA. Les indemnités viennent

réparer le préjudice subi par le client ou le prestataire lorsque l'autre partie est à l'origine du non-respect des SLA. Et si en tant que client Verizon, votre entreprise subissait par exemple une perte de CA de plusieurs dizaines de milliers d'euros pour cette opération de maintenance ?

Autres ressources :

- Attention : le cloud Verizon sera en maintenance pour 48h
- Le Cloud de Verizon à l'arrêt pendant 48h ce week-end
- Upcoming Verizon Cloud Downtime May Be Wakeup Call for Some
- Verizon has no excuse for its planned cloud outage