Formation CCSK / CCSP : retour d'expérience

Dans cet article, je vous propose un retour d'expérience sur une formation CCSK / CCSP que j'ai suivi en présentiel à Paris au mois de juin. Pour ceux qui souhaitent aller à l'essentiel, voici ici une synthèse de la formation et les enseignements à retenir.

Préambule

Comme certains d'entre vous le savent déjà, j'ai lancé récemment une nouvelle activité de formation en e-learning sur mes sujets de prédilection (Cybersécurité, sécurité Cloud, Blockchain, RGPD,…). Depuis le lancement de l'offre, j'ai reçu un nombre important de demandes pour des formations certifiantes du type CISSP ou Security+ et comme je m'intéresse depuis plusieurs années à la sécurité dans le Cloud, j'ai donc décidé de commencer par les certifications spécifiques à ce domaine à savoir le « Certificate of Cloud Security Knowledge » (*CCSK*) de la Cloud Security Alliance (CSA) et le « Certified Cloud Security Professional » (CCSP) de l'ISC^2. J'ai commencé ma préparation par de nombreuses recherches sur le Net et j'ai acheté la quasi-totalité des livres qui traitent du sujet y compris bien sûr le guide officiel de préparation au CCSP de l'ISC^2. J'ai également recherché les formations existantes en France dans le but d'analyser le marché et la concurrence. Je suis alors tombé sur une formation CCSK / CCSP sur 4 jours mais dont il est possible de suivre qu'une partie dite « avancée » qui se déroule sur 2 journées qui sont en fait les 2

derniers jours de la formation complète. Disposant d'un budget formation auprès de mon OPCO (FAFIEC), je me suis dit qu'il pouvait être intéressant de suivre cette formation avancée, d'une part pour compléter mes connaissances en la matière mais aussi et surtout pour me donner des idées sur l'approche pédagogique à utiliser pour enseigner la sécurité du Cloud dans une optique de certification. J'ai demandé un financement au FAFIEC qui a été accepté et j'ai donc suivi cette formation sur 2 jours à Paris en juin 2019 et c'est un retour d'expérience que je vous propose dans cet article. Comme l'expérience a été disons-le catastrophique, j'ai souhaité utiliser des noms d'emprunts pour les protagonistes. Ainsi la société de formation organisatrice s'appellera FORCLOUD et le formateur s'appellera Charlie. Précisons que Charlie est le patron de sa propre boîte et qu'il travaille en sous-traitance pour FORCLOUD.

Entrée en matière

En tout début de formation je demande s'il serait possible d'avoir une version électronique du support. Charlie me répond par la négative qu'il justifie pour des raisons de propriété intellectuelle (sic !) On reviendra plus loin sur ce support et cette fameuse propriété intellectuelle. On fait ensuite un tour de table où les participants (nous étions 4) se présentent. Lorsque vient mon tour, je me présente de façon tout à fait transparente en tant qu'expert en cybersécurité et actuellement en cours de préparation de modules e-learning CCSP et CCSK et là Charlie me dit « Ah ouais d'accord, tu es venu pour me piquer mes slides… ». Curieuse réflexion pour un formateur qui traite carrément son client de voleur dès les premières minutes de la formation. J'étais d'autant plus surpris qu'en tant que formateur depuis plus de 20 ans, j'ai toujours considéré que le savoir ça ne se vole pas, ça se partage.

Durée de la formation

Cette formation était commercialisée à un tarif de 2 420 € HT
pour une durée de 14 heures. Lors du dépôt de mon dossier de financement, mon conseiller FAFIEC m'avait fait remarquer que le tarif horaire était particulièrement élevé (173 € HT / H). J'avais alors argumenté en lui disant qu'il s'agissait d'une formation de haut niveau et que le tarif se justifiait. Mais quelle ne fut pas ma surprise en constatant les horaires du 1er jour (9h30-12h et

14h-16h30) et du 2ème (9h30-12h et 14h-16h) le tout agrémenté de 4 pauses de 15mn (une chaque matin et après-midi). En considérant le temps réel passé en formation, la durée a donc été de 8H30 ce qui nous fait une prestation de formation inter-entreprises à plus de 280 € HT / Heure. Alors à ce tarif bien sûr, on s'attend à ce qui se fait de mieux en matière de sécurité dans le cloud. Je précise qu'en fin de formation, j'ai rayé la mention 14h dans la feuille d'émargement et indiqué à la place 9h30. Dès lors CLOUDFORM était dans l'obligation de ne facturer qu'à hauteur de 67% du tarif (prorata-temporis de 9,5h / 14h) conformément à l'article 3 du contrat FAFIEC qui stipule : « *Conformément aux textes législatifs en vigueur, le FAFIEC ne règle qu'après exécution des prestations de formation et sur présentation des justificatifs s'y rapportant (Art. R6332-25 et Art. R6332-26 du code du travail). En conséquence, seules les heures effectivement réalisées sont réglées.* ».

Support de cours

Mais que contient donc ce fameux support de cours avec une telle valeur en matière de propriété intellectuelle qu'il est impossible de le donner en version électronique à des clients qui ont payé plus de 2 400 € leur formation ?

Sur la forme, le support est au format papier A4 avec 90 slides imprimés en noir & blanc. 45 slides par jour, c'est 3 fois moins que ce qui se fait généralement pour ce genre de formation (hors stage pratique). Sur le fond, le contenu est d'une pauvreté affligeante (nous y reviendrons plus en détail un peu plus loin). Environ 50% du support est constitué d'une multitude de copie de textes, dessins ou schémas en anglais avec la plupart du temps aucune mention de la source. Charlie a-t-il obtenu l'autorisation de plagier tous ces documents sans même mentionner leur auteur ? Le support n'est pas du tout autoporteur ce qui signifie qu'aucun slide ne comporte de phrases ou d'explications écrites de sorte que l'apprenant ne pourra jamais sans servir pour comprendre quelque chose qui lui aurait échappé lors des explications orales du formateur. Encore faut-il qu'il y ait une explication orale puisque Charlie a purement et simplement « oublié » de traiter environ une dizaine de slides… Le support ne comprend strictement aucun lien hypertexte pour accéder à des ressources complémentaires ni aucune référence bibliographique, même pas un bouquin pour préparer le CCSP ou le CCSK, c'est juste incroyable ! Conclusion et c'est un point positif, je suis finalement très content de ne pas avoir en ma possession la version électronique du document.

Contenu pédagogique

Dès les premières minutes, Charlie nous fait une présentation de la certification CCSK en indiquant les caractéristiques d'une version malheureusement dépassée (v3) et remplacée depuis juillet 2017 par la v4. Ensuite, un stagiaire lui demande le tarif de la certification et il ne connait pas la réponse qui bien sûr n'est pas mentionnée dans son support. Je m'interroge ainsi dès le début de la formation : « Comment peut-on prétendre préparer sérieusement à une certification quand on n'en connait même pas les caractéristiques les plus élémentaires ? »

Je ne vais pas ici rentrer dans le détail de la formation mais je dirais que l'on a couvert que très partiellement le programme CCSK / CCSP (env. 10 %). Il faut dire aussi qu'avec 8h30 d'enseignement réel, on ne peut pas aller bien loin. Chaque sujet a été abordé de façon totalement superficielle avec aucun exemple pertinent dans un contexte de Cloud. Prenons un exemple concret « la virtualisation des serveurs » : qu'avons-nous vu sur le sujet ? RIEN ! Pas la moindre identification d'une attaque par le soft (Hypervisor escape, VM hopping, VM sprawl,…) ou par le hard (Meltdown, spectre, Zombieload,…) ni même les problématiques du contrôle antiviral pour éviter un "AV Storm". Aucun exemple de POC sur ces attaques pour démontrer à des fins pédagogiques qu'elles ne sont pas que théoriques. Aucune recommandation en matière de sécurité pour durcir un hyperviseur ou pour réduire la surface d'attaque d'un environnement virtuel. Et puis bien sûr dans le support de cours, aucune ressource pour sécuriser la virtualisation et dieu sait qu'elles sont nombreuses (ANSSI-2013, CSA-2015, CIS-2015, ENISA-2017, NIST-2018,…) pour ne citer que ces quelques exemples. Pour tout cela RIEN à l'oral et RIEN à l'écrit. C'est ce que j'appelle une formation totalement creuse, où les sujets sont traités de façon superficielle avec strictement aucun exemple pratique ou cas d'usage réel. Charlie préfère visiblement parler pendant 30mn du chiffrement homomorphique que personne ne verra en production dans un datacenter avant 2040 (dans le meilleur des cas) plutôt que de parler de BYOK avec synchro de HSMs en mode hybride tellement plus efficace pour sécuriser les données dans le Cloud et opérationnel depuis déjà plusieurs années.

Au final dans ces 2 jours de formation, ma prise de notes s'est résumée à noter les erreurs, inexactitudes ou omissions du formateur. Prenons quelques exemples sur la conformité et les aspects juridiques :

- Je demande au formateur de nous parler du type 1 / type 2 des attestations SSAE16

non pas pour le piéger mais parce ce que c'est au programme du CCSP et Charlie me réponds : « Non, on ne voit pas ça ici » Dommage car non seulement cette différence n'est pas un détail mais en plus elle apparaît souvent dans les QCM de préparation à la certification.

- On aborde ensuite les certifications CSA, mais hélas ce que présente Charlie n'est plus du tout d'actualité et tout a changé depuis plusieurs mois pour intégrer la conformité RGPD et des options de certification continue mais Charlie n'est toujours pas au courant. OK je veux bien mais on est quand même à 100% dans le sujet de la formation et Charlie n'est pas « Up-to- date » dans une formation « avancée ». Avec un tarif horaire de 280 € HT, ça fait quand même cher l'information obsolète.
- On aborde ensuite le RGPD et Charlie n'as visiblement jamais entendu parler de Code de Conduite pour les fournisseurs Cloud. Alors je lui en parle et il me répond que ce n'est pas opérationnel alors que le CdC de la CSA date d'août 2018 et celui de CISPE depuis 3 ans. Par exemple AWS a adhéré au CdC CISPE avec certification tierce depuis février 2017 (soit 28 mois avant la formation).
- Charlies affirme qu'un audit sur site est obligatoire dans le cadre du RGPD. Je lui pose alors la question « Est-ce qu'un fournisseur qui refuse l'audit sur site à un client est en non-conformité avec le RGPD » et il répond sans la moindre hésitation : OUI. Alors voilà un nouveau Scoop, en juin 2019 (un an après l'entrée en application du règlement), Amazon, Micorosoft, Google, Salesforce, OVH et compagnie seraient toujours en non-conformité avec le RGPD. C'est bien évidemment tout à fait inexact. D'ailleurs voici, par exemple, ce qui est écrit dans ce qui se fait de mieux en matière de conformité RGPD dans le cloud à savoir le Code de conduite CISPE adopté par un centaine de fournisseurs IaaS dont AWS et OVH : Chapitre 4.6 (Demonstrating compliance) à la section b (Audit) : *« The Code does not require the CISP to authorise the customer or any third party to conduct an on-site audit of the CISP's premises or facilities. Cloud infrastructure services are multi-tenant environments. This means that the data of potentially all the CISP's customers could be hosted in the same premises or facilities. Physical access to the CISP's facilities by a single customer or third party introduces a potential security risk for all other customers of the CISP whose data is hosted within the same premises or facilities. This risk can be controlled if, instead of an on-site audit, customers use the information provided by the CISP to reasonably verify the CISP's compliance with the security obligations in the Service Agreement. »*
- Charlie évoque succinctement le Patriot act, qui au passage n'existe plus, sans parler de son successeur le Freedom Act ni du mécanisme d'application d'une NSL aux US ou en Europe.
- Rien non plus sur d'autres spécificités américaines comme FISA ou le « Privacy shield ».
- Charlie évoque le Cloud Act en oubliant de parler des « executive agreements » qui sont les éléments clés de ce mécanisme juridique sans lesquels il n'est pas utilisable. Rien non plus sur le conflit potentiel entre Cloud Act et l'article 48 du RGPD.
- Charlie évoques vaguement la notion de BCR pour finalement ne rien dire du tout

sur les conditions imposées par le RGPD sur les transferts hors UE. Les stagiaires vont donc partir sans savoir qu'un stockage dans un cloud non approprié pourrait coûter à leur entreprise 4% de leur CA ou 20M€.

- Mais pire que ça, le terme RGPD (ou GDPR) n'est même pas mentionné une seule fois dans le support de cours y compris dans la section juridique. C'est juste HALLUCINANT ! Pourtant, le GDPR est au programme CCSP et CCSK et Dieu sait qu'il y en a des choses à dire sur le sujet. Par exemple, dans ma formation sur la conformité RGPD dans le cloud computing, je délivre plus de six heures et demi de formation avec quelques 300 slides pour décrire tous les éléments de conformité. Comprenons-nous bien, je ne reproche pas à Charlie de ne rien m'avoir appris mais de ne pas avoir fait son boulot pour les 3 autres stagiaires.
- On ne parle pas dans la formation de la transposition de la directive NIS de 2016 dont la deadline pour les 28 pays membres était fixée 31 mai 2018 et avec elle toutes les obligations que cela impose aux fournisseurs de Cloud (FSN). C'est vraiment dommage cet oubli parce que c'est le seul et unique texte règlementaire qui s'applique directement et explicitement aux CSP. Trop récent encore un texte de mai 2018 pour une formation de juin 2019 ?
- Bien sûr on ne parle pas du tout des normes ISO/IEC spécifiques au Cloud dont la sortie date de 2014 (ISO 27018) et de 2015 (ISO 27017). Je n'attendais évidemment pas que Charlie nous explique les nouveautés de la 27018 dans sa révision de 2019.
- Bien entendu, comme Charlie occulte déjà les aspects juridiques qui sont au programme du CCSK et du CCSP (exemple : HIPAA pour la santé), il ne faut compter sur lui pour nous parler des spécificités françaises comme par exemple la certification HDS.
- Charlie n'aborde pas non plus le Cybersecurity Act dont le cadre de certification (en particulier le niveau substantiel) pourrait permettre de voir émerger les premières certifications européennes pour les fournisseurs Cloud dans l'UE.
- Pour finir, un participant interroge Charlie sur la Cyber-assurance à laquelle il répond par un exemple de rançongiciel sans rapport avec le Cloud. Je me permet alors de compléter en expliquant le rôle d'une cyber-assurance dans le Cloud qui permet de couvrir certains risques comme par exemple une sanction administrative de la CNIL. Et là Charlie me rétorque que c'est faux car des gens de la CNIL lui ont dit. Il va falloir que quelqu'un dise à Charlie que pour savoir ce que peut prendre en charge un contrat de cyber-assurance, on ne le demande pas à la CNIL (ni aux cybercriminels…) mais plutôt à une compagnie d'assurance. Ça lui évitera de dire de grosses bêtises.

Exercices et QCM d’évaluation

Au cours de la formation, Charlie nous a proposé plusieurs exercices dénués de tout intérêt pédagogique et dont le seul objectif semblait être : « gagner du temps ». Par exemple, dans le dernier exercice, Charlie demande à chaque stagiaire de choisir une mesure de sécurité dans la Cloud Controls Matrix (CCM) et de la transformer en questions à poser à un fournisseur. Très bel exercice qui demande aux stagiaires de réinventer la roue, puisque ce travail a déjà été réalisé par la CSA (questionnaire CAIQ) et au passage cela permet à notre ami Charlie de se reposer un peu et de vaquer à ses occupations pendant plus de 20 minutes. Ah oui, j’oubliais les 8h30 de formation, c’est avec les 3 exercices et les 2 QCMs. Si l’on ne comptabilise que le temps où Charlie anime véritablement la formation, on tourne aux alentours de 7 heures (on passe maintenant à 345 € HT l’heure de formation).

Terminons ce débriefing de la formation de notre ami Charlie en parlant du QCM proposé en fin de formation. Ça peut paraitre une bonne idée de faire passer un QCM à des stagiaires qui préparent une certification basée justement sur un QCM (Bien qu’il serait préférable que cela se fasse en dehors du temps de formation). Le QCM que nous propose Charlie est constitué de 18 questions toutes intégralement copiées soit sur des ouvrages de préparation au CCSP soit sur des sites Internet ce qui en fait une violation de propriété intellectuelle. Charlie est tellement soucieux de protéger sa PI, qu’il ne donne pas ses slides aux clients qui ont payé sa formation mais par contre il n’hésite pas à copier (sans payer, ni même mentionner la source) des questions qu’il utilise sans gêne dans une formation payante. Ce formateur ne manque visiblement pas de cran ! Ensuite, on passe 30 minutes à répondre à 18 questions et lors de la correction Charlie se contente de donner une rapide explication à seulement 5 des 18 questions. Doit-on lui rappeler qu’à son tarif horaire, son plagiat de 18 questions revient à 150 € pour chaque stagiaire. Charlie doit certainement savoir que pour 25€ sur Amazon, on peut acheter le livre « CCSP Official ISC^2 Practice Tests » qui propose 1 000 questions avec 1 000 réponses explicatives détaillées ? 55 fois plus de questions toutes corrigées pour un prix divisé par 6, qui dit mieux ? Où est la valeur ajoutée de ce QCM pour quelqu’un qui veut préparer la certification ? Dans cet exercice, mon voisin de droite qui n’a eu que 40% de bonnes réponses. Mais avec seulement 5 réponses expliquées, qu’a-t-il vraiment appris avec ce QCM ?

Synthèse de cette formation CCSK / CCSP

- 7h de formation effective pour une durée annoncée de 14h
- Tarif exorbitant de 345 € HT / heure
- Environ 10% du programme traité en distillant quelques informations sur le sujet qui seront au choix (non exclusif) : inexactes, dépassées, imprécises ou incomplètes
- Support de cours d'une pauvreté affligeante avec aucune référence externe
- Exercices dénués de tout intérêt pédagogique
- Nombreux sujets importants non abordés : BYOK, SDN, GDPR, Fédération d'identité,…
- Formation 100% théorique avec strictement aucune illustration pratique
- QCM intégralement pompé sur Internet avec 5 questions corrigées sur 18.

Conclusion

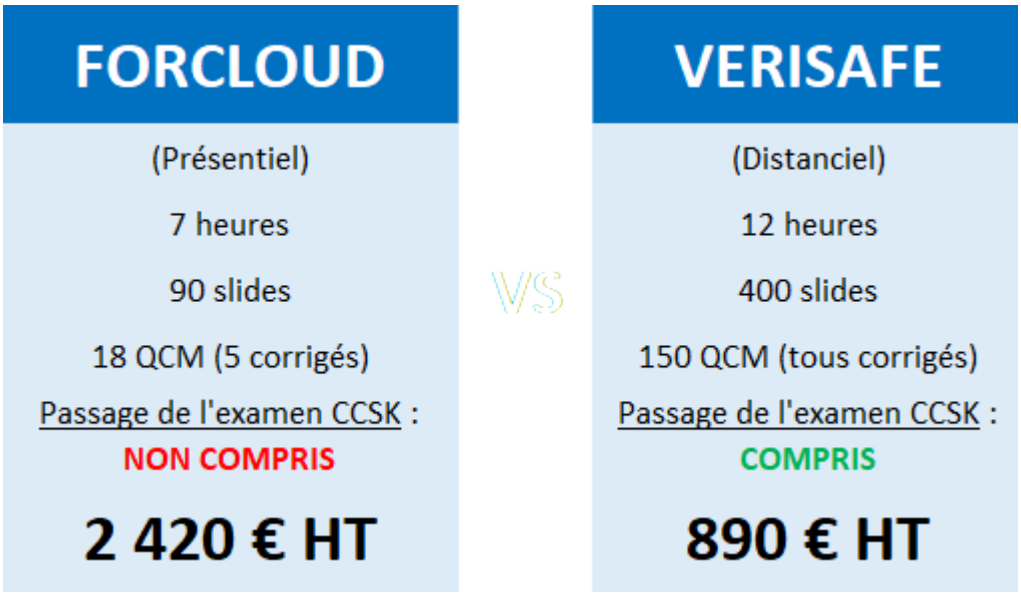
Je n'aurai jamais imaginé en m'inscrivant à cette formation que son seul intérêt serait de me donner matière à écrire un article sur cette triste expérience. J'ai bien entendu fait part de mon mécontentement au formateur par un retour détaillé adressé par email dès le lendemain de la formation. J'ai aussi demandé et obtenu que l'organisme de formation ne facture pas cette formation au FAFIEC. Même si cela ne coûtait absolument rien à ma société puisque la prise en charge était de 100%, j'en ai fait une affaire de principe dont je tire les 2 enseignements suivants :

(1) Concernant les questions

La qualité des réponses aux questions ne dépend absolument pas du type de formation (présentiel vs distanciel) mais de la compétence et de la motivation du formateur. On dit souvent qu'un des gros avantages du présentiel par rapport au e-learning c'est que l'on peut poser des questions et avoir tout de suite des réponses. Dans la formation dont il est question ici, je n'ai finalement posé que 2 questions : La première portait sur les différences dans SSAE16 entre type 1 et type 2 et on m'a répondu que ce n'était pas au programme (ah bon ?) et la deuxième était sur la conformité RGPD et la réponse était inexacte. Alors, oui les stagiaires aiment bien avoir des réponses à leurs questions. Mais à votre avis que préfèrent-ils ? Qu'on ne leur réponde pas ou qu'on leur donne des mauvaises réponses ou au contraire qu'on leur réponde avec exactitude et précision même si la réponse n'arrive pas dans la minute ?

(2) Concernant le tarif

On le sait, le tarif d'un produit ou d'un service ne fait pas sa qualité. Mais ici, soyons factuels ! En partant des horaires on obtient 9h30 de présence mais en enlevant tous les moments où le formateur ne dit pas un mot (pauses, exercices et QCM), on arrive à 7 heures d'animation effective. Avec une formation tarifiée à 2 420 € HT, l'animation coûte donc (pour chaque participant) 345 € HT de l'heure. Tarif qu'il faut bien sûr remettre en perspective avec le programme traité superficiellement et saupoudré d'informations inexactes, dépassées, imprécises ou incomplètes. Pour information, au moment où j'écris ces lignes, je suis en train de réaliser pour VERISAFE une formation de préparation à la certification CCSK en E-learning dont les caractéristiques (non définitives) seront les suivantes : 12 heures de formation, 400 slides, 150 QCM.

- 

En conclusion, je pense qu'il est impossible d'obtenir la certification CCSK après avoir suivi cette formation en présentiel sur 2 jours (et même en ayant suivi la session de 4 jours avec ce formateur) et je ne parle même pas de la certification CCSP de l'ISC² qui est encore plus difficile à obtenir. En ce qui me concerne, cette expérience me motive encore plus à vouloir produire des formations de qualité pour donner à chacun le maximum de chance de réussir leur certification (CCSK, CCSP ou CISSP).

Le référentiel ANSSI SecNumCloud

Le référentiel de qualification des prestataires de services d'informatique en nuage (SecNumCloud) vient enfin d'être publié par l'ANSSI. Qu'apporte t-il par rapport à une certification ISO 27001 ? Donne t-il toutes les garanties de sécurité attendues par les clients ?
Nous vous proposons une analyse détaillée de ce référentiel avec en particulier un focus sur 50 exigences. Au-delà de la qualification des prestataires, découvrez comment SecNumCloud peut vous permettre d'évaluer la sécurité de vos fournisseurs.

Sommaire de la présentation

La vidéo d'environ 45mn ainsi que les slides de la présentation sont réservés aux membres enregistrés sur le blog. N'hésitez pas à vous inscrire gratuitement ou utiliser votre compte LinkedIn, Google, Microsoft, Twitter ou Facebook pour pouvoir y accéder.
Pour les personnes non inscrites, un extrait de la présentation est disponible ici.

Les slides de la présentation

Numergy c’est fini

Après une mise sous procédure de sauvegarde le 13 octobre dernier, SFR vient de procéder au rachat de l’intégralité du capital de Numergy. Dans un communiqué de presse publié hier, Michel Combes, PDG de SFR déclare : *« Ce rapprochement s’intègre à la stratégie Entreprise du groupe Altice dont l’une des priorités est de consolider l’ensemble de ses activités autour du Cloud, de l’IOT et des services managés. »*

Il faut se rappeler le projet de Cloud souverain français (Andromède) émane d’un appel d’offres lancé en 2010 dans le cadre des « investissements d’avenir » et que pour des raisons essentiellement politiques, il a donné naissance à deux sociétés Cloudwatt et Numergy. La fin de Cloudwatt est actée depuis un an (rachat par Orange), c’est donc maintenant au tour de Numergy de subir le même sort. Mais pouvait-il en être autrement ?

Dans cette affaire de Cloud souverain beaucoup d’erreurs ont été commises. Celles du gouvernement français tout d’abord. On ne peut en effet que s’interroger :

- Pourquoi financer deux startups concurrentes sur un même marché ?
- Comment peut-on imaginer qu’avec un capital de 225 M€ non entièrement libéré, un nouvel entrant puisse rivaliser face à des géants américains déjà opérationnels et qui continuent leurs investissement à coup de milliards d’euros ?
- Pourquoi n’y a-t-il eu aucune volonté politique pour instaurer une véritable dynamique Cloud auprès des administrations et collectivités locales à l’image du Cloud first Policy instauré aux états-unis ?
- Pourquoi ne pas raisonner à l’échelle européenne avec des produits de sécurité exclusivement européens ou open source afin de revenir un tant soit peu vers la notion de souveraineté ?

Bien sûr Numergy a également commis des erreurs sur le plan commercial, marketing et technologique mais dans un contexte pareil, comment leur en vouloir ? Qui aimerait travailler dans une société dans laquelle les 3 principaux actionnaires ne s’entendent pas, n’ont pas les mêmes intérêts ni les mêmes objectifs et n’ont pas la même vision stratégique du business ?

Pourtant en matière de sécurité, Numergy avait fait beaucoup d’effort. On peut citer par exemple :

- Une excellente redondance via 5 datacenters Tier 3 situés en France,

- Une offfe « Numergy Santé » agrée officiellement par l'état en tant qu'hébergeur de données de santé (HDS),
- Une certification ISO 27001:2013 délivrée par le BSI,
- Une certification CSA STAR Silver délivrée également par le BSI.

Comme quoi dans le Cloud, la sécurité est une condition nécessaire (et même indispensable) mais pas suffisante pour s'imposer sur le marché. Le rachat de Numergy signe ainsi la fin des ambitions de l'Etat français dans son projet de Cloud souverain. Reste maintenant à savoir ce que le groupe Altice va faire de cette activité Cloud.

AWS : « surprenante » certification ISO 27017

Chad Woolf, Directeur risques et conformité chez AWS, a déclaré le 30/11/2015 sur le blog officiel d'Amazon : "*I am happy to announce that AWS has achieved ISO 27017 certification*".

Cette annonce est pour le moins surprenante car contrairement à l'ISO 27001, la norme ISO 27017 ne décrit pas un processus de gestion mais fournit un guide de bonnes pratiques. Elle a été développée par l'ISO pour compléter le guide initial définie par l'ISO 27002 et propose un ensemble de mesures de sécurité destinées à améliorer la sécurité des services dans le cloud.

En pratique, AWS a réactualisé son SMSI (pierre angulaire de l'ISO 27001) et mis à jour sa DdA (Déclaration d'Applicabilité) en adoptant les bonnes pratiques de l'ISO 27017. AWS a ensuite demandé à Ernst & Young de procéder à un nouvel audit pour attester de la prise en compte de l'ISO 27017 dans sa démarche ISO 27001.

On peut ainsi lire dans le certificat 27017 d'AWS : *" … certified under certification number [2013-009], is also compliant with the requirements as stated in the standard : ISO/IEC 27017:2015 "*
(*pour information, le numéro de certification [2013-009] correspond au certificate ISO 27001 d'AWS)*

En d'autres termes, Ernst & Young atteste que le SMSI d'AWS prend en compte les bonnes pratiques issues de l'ISO 27017 ce qui n'apporte en soi aucune information précise sur le niveau de sécurité effectif du fournisseur. En effet, en l'absence de

publication de la DdA, on ne sait strictement rien sur la façon dont les mesures de sécurité proposées par l'ISO 27017 sont réellement implémentées au sein du SMSI d'AWS. Il s'agit donc encore une fois d'une démarche purement marketing, destinée à rassurer le client perdu dans la jungle des normes ISO/IEC 270xx. Dans le même état d'esprit, AWS aurait pu également demander à Ernst & Young un certificat ISO 27002 puisque naturellement son SMSI s'appuie sur des mesures issues de l'ISO 27002. Et pourquoi ne pas demander dans la foulée un certificat ISO 27005 puisque l'analyse de risque effectuée par AWS s'appuie sur ce référentiel ?

Le référentiel de l'ANSSI se fait attendre

Mais que diable fait l'ANSSI avec le document que tous les acteurs français du Cloud attendent avec impatience : Le référentiel de qualification de prestataires de services sécurisés d'informatique en nuage.

Suite à la diffusion de la dernière version de travail (v1.3) le 20 juillet 2014, l'ANSSI avait lancé un appel à commentaires avec une date de clôture fixée au 3 novembre 2014. Cela fait donc bientôt un an que cette « dead line » est passée et depuis silence radio ! Combien de temps faudra-t-il encore à l'ANSSI pour prendre en compte les différentes remarques et les autres initiatives (Secure Cloud, Cloud confidence) et publier un référentiel définitif ?

Le référentiel de qualification de l'ANSSI contient des exigences et recommandations à destination des prestataires de services d'informatique en nuage. La qualification permet d'attester de la conformité du prestataire aux exigences du Référentiel. Pour cela, un organisme de qualification désigné par l'ANSSI est chargé de vérifier que le prestataire respecte les exigences (chapitres 5 à 18) par un audit du prestataire. Concernant les recommandations indiquées dans le référentiel, elles sont données à titre de bonnes pratiques et ne font l'objet d'aucune vérification en vue d'obtenir la qualification.

Le référentiel propose deux niveaux de qualification des prestations de *cloud* :

- le premier niveau, dit élémentaire, est conçu pour offrir un niveau de protection équivalent à celui requis par la PSSIE
- le second, dit standard, qui offre une protection plus robuste et permet notamment d'envisager le traitement de données sensibles de niveau Diffusion

Restreinte.

Que peut-on dire de la version v1.3 diffusée par l'ANSSI le 20 juillet 2014 ?

Globalement, ce référentiel est assez décevant. On a l'impression qu'il a été rédigé en réalisant une adaptation de la norme ISO 27002 à la problématique de sécurité dans le Cloud. D'ailleurs, la structure du référentiel est un véritable copier/coller de la norme ISO 27002.

Pour ma part, j'ai formulé les remarques suivantes :

- Il n'y a aucune distinction effectuée entre les différents prestataires (IaaS, PaaS et SaaS) malgré les différences fondamentales en matière de sécurité et de responsabilités entre prestataires et clients,
- Il n'est fait aucune référence aux normes ISO internationales relatives au Cloud (ISO 17788, 17889, 27017, 27018). Même si ces normes sont très récentes, les drafts sont disponibles depuis très longtemps,
- Il n'y a aucune exigence concernant la disponibilité minimale des services,
- Il n'y a aucune exigence concernant la réversibilité des données (mesure totalement indispensable à la maitrise des données externalisées),
- Il y a par contre de très forte exigence nationale (localisation des données exclusivement sur le territoire français, support de premier niveau francophone localisé en France, contrat de droit français, tribunal compétent français, etc…) à tel point que l'on ne comprend pas comment l'ANSSI peut parler d'un référentiel ouvert doté d'une ambition européenne.

Les plus optimistes ont le droit de penser que l'ANSSI a bien pris en compte toutes les remarques formulées par les différents contributeurs et qu'un tout nouveau référentiel devrait sortir dans les prochains jours. Wait and see…

Cheops Technology certifié ISO 27001

Après Numergy, Outscale et OVH, un nouveau fournisseur de Cloud français, Cheops Technology, vient d'obtenir la certification ISO 27001. A cette occasion, Nicolas Leroy-Fleuriot, PDG de l'entreprise, déclare dans un communiqué de presse diffusé aujourd'hui :

«Les opérateurs de Cloud doivent rassurer leurs clients en validant des

certifications de pointe en matière de sécurité, telle la certification ISO 27001 qui est une norme drastique en matière de sécurité des Systèmes d'Information»

Les fournisseurs se servent en effet de toutes les certifications de sécurité disponibles pour rassurer leurs prospects ou clients qui n'ont bien souvent qu'une vague connaissance de ces certifications. Peut-on par exemple dire que l'ISO 27001 est une norme drastique en matière de SSI ? Rappelons qu'une certification ISO 27001 ne garantit en aucun cas un bon niveau de sécurité. Elle ne donne également aucun élément pour réaliser une analyse de risques pertinente et ne garantit pas non plus la pertinence des solutions de sécurité mises en œuvre. En fait, la norme ISO 27001 atteste simplement que l'organisme a mis en œuvre un processus de gestion de la sécurité de son système d'information (SMSI) conforme à la politique de sécurité qu'il a lui-même défini. Elle ne certifie donc en aucun cas que le SI du fournisseur et les données de ses clients sont correctement sécurisés.

Autres ressources :

- Cheops Technology : CP ISO 27001