Comment garantir la sécurité du Cloud public

Retentissantes affaires de piratage, pannes médiatisées, risques d'espionnage économique : **le Cloud public apparaît comme risqué** à plus d'un titre aux yeux d'un DSI. Pourtant, à tête froide, ce type de déploiement ne présente pas, sur certaines plans, plus de risques que des architectures plus classiques. Les pannes, surtout, sont plus fréquentes dans les propres datacenters des entreprises.

D'autant qu'**il existe aujourd'hui des bonnes pratiques pour sécuriser ses données** placées dans le Cloud public. En commençant par mettre en place une vraie gestion des accès à ces services, via par exemple un outil dédié permettant de centraliser les mots de passe ou via l'emploi systématique de la double authentification. Limiter l'accès à des adresses IP correspondant à l'intranet de l'entreprise constitue une autre façon de limiter les risques. Sans oublier évidemment le cryptage des données déposées dans les nuages. Autant d'exigences qui pousseront l'entreprise à fouiller dans les options des différents fournisseurs.

Au-delà des aspects techniques, sécuriser son Cloud public passe aussi par un certain nombre de **démarches vis-à-vis des prestataires**, afin de se prémunir d'éventuels dysfonctionnements. Un domaine bien moins balisé, où il faut se frotter aux contrats standardisés des grands prestataires de Cloud américains, aux clauses ubuesques en matière de récupération de données. Des domaines où l'assistance des SSII se révélera bien utile, pour ne pas dire indispensable.

Découvrez dans notre dossier des solutions pratiques pour sécuriser les initiatives Cloud des différents métiers de votre organisation.

Dossier réalisé par Yann Serra

Avec le Cloud public, les applications, les documents et mêmes les serveurs sont accessibles par Internet. Problème, Internet est notoirement sensible aux vols de données, aux pannes, à l'espionnage. Parmi les braquages les plus retentissants, **77 millions de coordonnées bancaires ont été extraites du Playstation Network** en avril 2011, les mots de passe de 38 millions de comptes utilisateurs ont été volés, ainsi que les codes sources de tous les logiciels Adobe depuis le site de l'éditeur en octobre 2013. Apple et Canonical (Ubuntu Linux), qui conçoivent pourtant des systèmes a priori inviolables, se sont également fait dérober les mots de passe de certains de leurs comptes utilisateurs, respectivement 100.000 et 1,8 millions, en juillet dernier. Plus proches de nous, ce sont 800 000 coordonnées clients qui ont été extraites depuis le site d'Orange en janvier dernier.

Avec les identifiants dérobés, les pirates peuvent accéder ensuite aux informations que chaque utilisateur a stocké en ligne, pour les exploiter ou les détruire. Bien sûr, chaque fournisseur se défend en expliquant que les mots de passe dérobés étaient toujours cryptés. Il faudrait donc des siècles et beaucoup de puissance de calcul pour décoder les clés de tous les comptes. Certes, mais il ne faut que quelques heures pour décoder celle d'un seul compte.

Piratages et pannes ultra-médiatisés

En ce qui concerne les pannes, des incidents de nature logicielle ou matérielle se produisent régulièrement et affaiblissent la disponibilité des données. Citons les défaillances de Microsoft Azure survenues en février 2012 puis en février 2013, les pannes à répétitions pour Salesforce durant l'été 2012, l'ouragan Sandy qui a douché en octobre 2012 les centres de données de la côte est des États-Unis et, par ricochet, les infrastructures d'Amazon et de Google. Google, d'ailleurs, dont toutes les applications en Cloud se sont mises à dysfonctionner le 24 janvier dernier à cause, cette fois-ci, d'un bug logiciel dans son infrastructure. Le 17 août dernier, c'était à cause d'une erreur humaine dans la mise à jour des systèmes. Et puis, les pannes peuvent aussi être provoquées par un acte de piratage. C'est ce qui est arrivé le 16 février dernier au service en ligne CloudFlare, lequel a succombé sous une attaque massive de déni de service. Ironie du sort, CloudFlare est censé être un Cloud de sécurité qui protège les sites webs des utilisateurs qui s'y abonnent… Selon l'International Working Group on Cloud Computing Resiliency, qui référence toutes les pannes, **les 13 premiers fournisseurs mondiaux ont cumulé 600 heures d'indisponibilité** sur les cinq dernières années.

Quant à l'espionnage, l'affaire Prism a prouvé que les fournisseurs de services en ligne américains pouvaient **accéder aux contenus déposés par leurs clients sur demande de l'état**. Autant dire qu'ils peuvent y accéder tout court. Un DSI qui préfère garder l'anonymat témoigne ainsi avoir voulu changer de prestataire pour son service d'e-mail dans le Cloud et a donc sollicité des concurrents par… e-mail. « *Quelle ne fut pas ma surprise de recevoir un coup de fil de mon prestataire pour me dire qu'il s'alignait sur l'offre la plus compétitive, alors qu'il n'était officiellement pas au courant que nous voulions en changer.* » A l'évidence, ce prestataire avait fouillé dans la messagerie dont on lui avait confié la garde.

Pourtant, le Cloud public n'est pas plus risqué

Malgré tout, le Cloud public n'est pas plus dangereux qu'un centre de données cadenassé dans le sous-sol d'une entreprise, ou qu'un Cloud privé non accessible depuis Internet. Pour preuve, en juillet 2013, OVH a aussi été la victime d'un piratage de sa base utilisateurs qui a permis le vol 700 000 identifiants. Sauf qu'il ne s'agissait pas du tout ici de Cloud public. Juste de l'hébergement de serveurs physiques ou virtuels sur un réseau privé. En fait, pour agir, **les pirates n'ont pas besoin que leur cible soit sur Internet**. La clé de leurs braquages est le mot de passe d'un utilisateur légitime, souvent obtenu par le biais d'un site de phishing (faux portail web dont la visite urgente est incitée par un e-mail catastrophiste) ou via un cheval de Troie (virus envoyé par e-mail pour prendre possession du PC de l'utilisateur). Avec ce mot de passe, les pirates attaquent un système où qu'il se trouve, qu'il soit sur un réseau privé ou non.

Les pannes, surtout, sont plus fréquentes dans les propres datacenters des entreprises. C'est ainsi que **Julien Chambert**, le directeur Gestion, Supports et Systèmes d'Avexia Voyages, n'hésite plus à faire héberger dans le Cloud public d'Amazon des applications sensibles, notamment celle qui sert aux professionnels à enregistrer les réservations de billets. « *Avec ce Cloud, nous avons aujourd'hui de meilleurs taux de disponibilité de nos données et de nos applications que lorsque notre informatique fonctionnait en interne, de manière artisanale,* » témoigne-t-il. Quant aux **prestataires professionnels**,

il n'y aucune raison qu'ils soient plus à l'abri des erreurs humaines que les géants Google ou Amazon. En mai 2011, l'arrachage de fibres optiques par une pelleteuse lors de travaux sur la chaussée à Vélizy-Villacoublay, en région parisienne, a rendu indisponibles pendant plusieurs jours les applications et les données stockées dans les Cloud privés de l'hébergeur Prosodie. Celui-ci s'était bien targué auprès de ses clients d'utiliser une double connexion fibre pour assurer la continuité du service si l'une d'elle était coupée. Mais il ne s'était pas rendu compte que les deux fibres passaient par le même fourreau.

En matière d'espionnage, c'est pareil. Le représentant d'un éditeur de logiciels de sécurité, qui tient aussi à témoigner de manière anonyme pour ne pas froisser ses clients, relate que dans 100% des entreprises ou des prestataires, il y a toujours un informaticien qui cède à la tentation d'aller lire les données des utilisateurs (e-mails, documents) grâce à son mot de passe administrateur. En clair, moins votre prestataire a de clients, plus vous avez de risques que cela tombe sur vous.

Et **Louis Naugès**, le co-fondateur de cabinet de conseil Revevol, de conclure que tout le mal qu'on veut bien entendre sur la sécurité du Cloud public serait **de la propagande, entretenue par les vendeurs de serveurs** (HP, Dell…), **les fournisseurs de réseau d'entreprise** (Cisco…) et **les éditeurs de logiciels d'infrastructure** (CA, HP, Microsoft, VMware…). « *Les seuls pour qui le Cloud public représente un danger, et même un danger mortel, ce sont les fournisseurs traditionnels »,* explique-t-il. Et d'ajouter que cette propagande serait particulièrement audible auprès de certains DSI *« qui mesurent leur pouvoir à la taille de leur centre de calcul.* »

4 bonnes pratiques pour ne pas se faire pirater son Cloud public

Il n'existe **pas de cas connu de piratage d'un service de Cloud public** lui-même. En revanche, les comptes utilisateurs hébergés sur un Cloud public sont attaqués de la même manière que les comptes utilisateurs hébergés sur les serveurs d'un datacenter privé : il suffit au pirate d'obtenir le bon mot de passe. Dans le cas de l'e-mail et de la bureautique, par exemple, il n'y a qu'à s'identifier correctement sur le portail du service pour accéder à tous les messages du compte, qu'importe que ce portail soit celui du VPN mis en place en interne pour les salariés ou celui du service en Cloud public Office 365 de Microsoft.

1/ Ne laissez plus fuiter vos mots de passe avec Dashlane

Qu'il s'agisse d'une application sur Internet (SaaS), de stockage en ligne ou de machines virtuelles (IaaS), un compte dans un Cloud public s'accède grâce à un identifiant (généralement votre adresse e-mail) et un mot de passe. La première bonne pratique consiste à avoir **autant de mots de passe différents que de comptes dans des Cloud publics** et il faut que ces mots de passe soient très complexes. C'est-à-dire avec plus d'une dizaine de caractères où se mélangent minuscules, majuscules, chiffres et ponctuations. Or, dans pareille configuration, tous ces mots de passe deviennent pratiquement impossibles à retenir. L'erreur à ne surtout pas commettre est de les noter dans un fichier ou sur un post-it pour s'en souvenir : il suffirait dès qu'on vous dérobe ce document pour avoir accès à tous vos comptes.

Une solution existe : le logiciel Dashlane, compatible Mac, PC et mobiles iOS comme Android. Lorsqu'il est activé, Dashlane génère **un nouveau mot de passe aléatoire et très complexe** à chaque fois que vous vous inscrivez sur un nouveau service en ligne. Il les garde en mémoire dans un fichier crypté et remplit automatiquement les champs d'identification à chaque fois que vous connectez à nouveau à un service. Il peut de surcroît être programmé pour se désactiver au bout de quelques minutes, voire ne fonctionner que lorsque l'utilisateur le lance, en cochant son bouton en forme de cerf qui s'est installé dans la barre de fonctions de tous les navigateurs web. L'astuce est que Dashlane ne s'active que lorsque vous entrez **un mot de passe maître**, finalement le seul qu'il soit nécessaire de retenir.

Dashlane est gratuit. Mais il existe une version payante, à 29,99 €/an, qui a l'avantage de partager les mots de passe de vos comptes entre tous vos appareils.

2/ Privilégiez la double authentification

La seconde bonne pratique consiste à **ne s'abonner qu'à des services de Cloud public qui utilisent le nouveau système d'authentification en deux temps**. Avec ce système, le service en ligne s'aperçoit quand l'utilisateur essaie de se connecter avec un ordinateur ou un mobile différent de d'habitude. Ce qui sera le cas d'un hacker qui a eu connaissance de votre mot de passe et qui tente de se connecter sur votre compte depuis sa machine. Le service en ligne demande alors de saisir un code supplémentaire pour entrer. Code qu'il envoie au titulaire du compte par SMS. Si le pirate ne vous a pas volé votre téléphone portable, il est peu probable qu'il devine ce code, généré aléatoirement et valide uniquement pendant quelques heures.

Google, Microsoft, Salesforce, Amazon AWS, Dropbox (Cloud public de stockage en ligne) et le français OVH supportent cette fonction de double authentification, mais ce ne sera vraisemblablement pas le cas du tout venant des services en ligne. Heureusement la plupart des applications SaaS en Cloud public permettent de se connecter en utilisant l'identifiant dont on se sert chez Google (Gmail, GoogleDrive, Google+, etc.), ce qui a pour effet d'activer la fonction de double authentification de celui-ci. Sont également souvent rencontrés sur le Cloud public les identifiants des comptes Facebook, LinkedIn ou encore Apple. Enfin, le service en ligne www.symplified.com, sur lequel on se connecte par double authentification, peut servir d'intermédiaire vers la connexion à n'importe quelle application SaaS. Évidemment, pour un maximum de sécurité, il s'agit d'abord de se connecter à un service de double authentification au moyen de Dashlane.

En ce qui concerne les abonnements professionnels à un service en ligne, qui comprennent un accès par salarié, attention à bien **vérifier que la fonction de double authentification est cochée pour tout le monde** dans la console d'administration (de Google Apps for Business, en l'occurrence, ou de symplified.com). Cela suppose que la personne qui gère l'abonnement groupé puisse renseigner pour chaque utilisateur un numéro de téléphone apte à recevoir un SMS.

Étonnamment, les Cloud publics français Numergy et Cloudwatt ne supportent toujours pas la double authentification.

3/ Dotez le Cloud public d'un accès privé

Les Cloud publics qui donnent accès à des serveurs virtuels en ligne (IaaS) ne permettent

généralement pas de s'identifier avec un compte Google ou Symplified. Dans ce cas, l'idéal est **configurer tous les serveurs virtuels** qui ne serviront pas à afficher votre site web **sur un réseau privé (VPN)**, c'est-à-dire avec des adresses IP inaccessibles depuis Internet car elles correspondent à la plage d'adresse de l'intranet de votre entreprise.

Les Cloud IaaS publics d'Amazon (EC2), de Microsoft (Windows Azure), d'IBM (SmartCloud) offrent cette option. En revanche, les Cloud IaaS publics français ne l'ont pas. A la place, les Security blocks d'OVH et l'interface SelfCare de Numergy permettent de restreindre l'accès de vos serveurs virtuels à une liste prédéfinie d'adresses IP publiques. Typiquement, il s'agira de l'adresse IP publique de la passerelle Internet de votre entreprise.

Attention : contrairement aux applications en SaaS et aux offres de stockage en ligne avec lesquels les échanges sont toujours cryptés (en SSL, via le navigateur), la communication avec des serveurs virtuels se fait en clair. Il est donc nécessaire d'**activer sur les machines virtuelles le protocole d'accès à distance crypté SSH**, typiquement au travers de l'outil gratuit OpenSSH (disponible pour les serveurs virtuels Windows et Linux).

Si cela fonctionne pour les Cloud publics de type IaaS, il est à noter que la connexion en VPN entre le réseau local de l'entreprise et un service SaaS (applications en ligne) n'est pas spontanément disponible. Pour que cela soit possible, il faut que la DSI de l'entreprise parvienne à contacter l'éditeur de l'application SaaS, afin de mettre avec lui en place un tel moyen de connexion. Ainsi, il deviendra par exemple possible de se connecter à une application SaaS au moyen de l'annuaire interne de l'entreprise, LDAP ou ActiveDirectory. La remarque n'est pas anodine : **installer un accès privé vers un service SaaS restaure le rôle de la DSI** dans l'entreprise, alors que la démocratisation du Cloud public a tendance à inciter les métiers à se passer de leur DSI.

4/ Cachez les informations stockées en ligne

Dans le cas d'un service de stockage en ligne, une troisième bonne pratique est de **crypter toutes les données avant de les y déposer**. Le moyen le plus éprouvé est de passer tous les documents à la moulinette de TrueCrypt, un logiciel gratuit pour Mac et PC, **recommandé par l'ANSSI** (Agence Nationale pour la Sécurité des Systèmes d'Information). Pour l'anecdote, **TrueCrypt** est à ce point sécurisé qu'il supporte d'encoder dans le même fichier plusieurs dossiers, chacun accessible avec un mot de passe différent. L'éditeur du logiciel recommande, pour les informations les plus critiques, d'enregistrer dans le lot de fausses informations. De sorte qu'un pirate mettra encore plus de temps à casser tous les mots de passe et, au final, ne saura pas quelles sont les informations à retenir.

Quant au partage de documents entre utilisateurs, trois options existent sur tous les services de stockage en ligne : les mettre dans le dossier public de votre compte (à proscrire car on peut les retrouver en faisant une simple recherche Google), ne les rendre accessible que via une URL complexe (à proscrire car l'URL pourra avoir été récupérée) et **ne permettre leur accès qu'à une liste déterminée d'autres utilisateurs** du service (à privilégier car ces utilisateurs devront avoir réussi la double authentification). Les services de stockage en ligne les plus réputés sont DropBox, GoogleDrive et Microsoft SkyDrive (désormais appelé OneDrive) à l'international, ainsi que CloudWatt et OVH Hubic en France.

Comment se prémunir des dysfonctionnements du Cloud public

Si les prestataires de Cloud privés ne sont pas plus à l'abri des pannes que les éditeurs de services en Cloud public, ils sont néanmoins contractuellement tenus de dédommager leurs clients lésés. Dans le Cloud public, au contraire, les prestataires font **fi de toute responsabilité**. Qui plus est, les services étant en majorité américains, il est pratiquement impossible de les joindre en cas de problème. Finalement, la seule exigence qu'une entreprise peut réellement obtenir, c'est de ne travailler qu'avec des services Cloud dont l'hébergement a reçu la **certification ISO 27000**. Celle-ci précise que l'hébergeur a bien mis en place les normes de sécurité en vigueur pour contrer les pannes et le piratage. Dans la plupart des cas, les applications SaaS sont hébergées dans les Cloud publics d'Amazon, Google ou Microsoft, lesquels sont certifiés. Mais cette information n'étant pas souvent visible sur le portail des applications SaaS, il faudra la plupart du temps l'obtenir en envoyant un e-mail aux éditeurs du service. La présence de la norme ISO 27000 permet à l'entreprise de **faire jouer son assurance en cas de perte ou de piratage des données**.

1/ Passez par un sous-traitant pour endosser les responsabilités

Jérôme Jelocha, le DSI de ePressPack, a trouvé la solution pour contourner l'absence de contrat : moyennant un prix majoré d'environ 10%, il confie la responsabilité de ses abonnements SaaS et IaaS à un prestataire local. « *Je n'ai que faire des engagements indiqués au bas d'un service web le plus standardisé possible. Je veux travailler avec un maître d'œuvre. Alors, je passe par un intermédiaire, une société de service, qui se charge de garantir l'accès à mes données par contrat, ce que ne propose aucun éditeur d'application SaaS* », dit-il.

Google liste une série de revendeurs agréés en France sur son annuaire des partenaires. Microsoft a aussi le sien, ainsi qu'Amazon. D'une manière générale, toute SSII peut servir d'intermédiaire pour s'abonner à un service de Cloud public, à partir du moment où elle fait la preuve d'avoir reçu l'agrément de la part de l'éditeur du service. Pour trouver une SSII fiable, consultez l'annuaire en ligne des chambres de commerce et d'industrie, lequel valide les prestations de plus de deux millions de prestataires français. Vous pouvez vérifier les antécédents de votre sous-traitant en interrogeant le service en ligne de Kompass.

Parmi les options typiques qu'une société de service apportera, on trouve communément **la prise en charge de sauvegardes locales** des fichiers, pour récupérer ses données quoi qu'il arrive, et **la mise en place d'un VPN**, pour accéder aux services du Cloud public au travers d'une connexion cryptée et privée. Surtout, la SSII s'engage par contrat à **dédommager son client le cas échéant**. Mais attention : les dommages couverts par le contrat sont seulement ceux dont la SSII est responsable. Vous ne serez pas remboursé si Google tombe en panne, mais vous le serez si la SSII, en plus, ne parvient pas à vous rendre vos fichiers.

Le problème, surtout, est que personne ne sait vraiment quels contrats signer pour quels services de Cloud, qu'ils soient publics ou privés d'ailleurs. « *Les avocats en sont encore à apprendre sur le tas, avec les affaires en cours ; aucune bonne pratique n'a été actée par la jurisprudence* », explique **Arnaud Lefrançois**, directeur du service achats chez Exxelia (industriel de la Défense), qui planche en ce

moment sur ces questions avec les professeurs de droit de HEC. A défaut de mieux, pour rédiger le contrat qui vous lie au prestataire, reportez-vous à la norme ISO/CEI 27002:2013 (lecture payante) qui liste les responsabilités d'un sous-traitant informatique. Le site Avocat Online publie également une liste des exigences à stipuler dans un contrat de Cloud.

2/ Préparez-vous à souffrir pour récupérer vos données

Parmi les vides juridiques figure la récupération des informations mises dans le Cloud. À l'heure actuelle, aucun fournisseur de Cloud public ne s'engage à restituer les données à la clôture du contrat – à part Salesforce, mais juste dans un délai de 30 jours – et encore moins dans un format compatible avec un service concurrent. En clair, il y a toujours moyen de télécharger les informations en cours de route, soit dans un format générique (.DOC, .XLS…), soit dans un format XML plus ou moins indexé, soit dans un format brut .CSV, où toutes les informations sont juste écrites les unes à la suite des autres. « *Nous avons testé dès le début que nous pouvions récupérer nos informations au format XML. Mais notre difficulté est qu'il n'existe pas deux ERP en SaaS qui aient les mêmes fonctions sur les mêmes données* », s'indigne **Christophe Chapet**, le DSI de l'office immobilier Nantes Habitat, qui se désole de ne pouvoir changer simplement d'outil de monitoring de son activité.

Pour **migrer entre deux applications SaaS**, il faut donc **nettoyer à la main les données récupérées**, les réordonner, les **mettre dans un format spécifique** avant de pouvoir les utiliser à nouveau. « *Le transfert de 800 comptes e-mails du Cloud de Microsoft (Office 365) à celui de Google (Gmail) nous a ainsi pris quatre mois* », témoigne Jérôme Jelocha. La **migration des documents bureautiques entre Office 365 et Google Docs**, le cas le plus simple, occasionnera des **dégradations** dans les mises en page, voire la perte des macros. En revanche, impossible de savoir si les données exportées par Salesforce concernent un suivi clientèle, un bilan comptable ou un dossier RH. Encore une fois, la sortie d'une offre de Cloud public et la migration vers une autre sont des tâches à confier à une SSII, laquelle engagera sa responsabilité par contrat.

L'ETSI (European Telecommunication Standards Institute) est mobilisée depuis septembre dernier pour **définir les normes qui assureront l'interopérabilité et la portabilité entre applications SaaS**. Son groupe de travail, la Cloud Standard Coordination, est censé présenter ses premiers résultats en juin prochain. Mais peu d'informaticiens y croient : « *ce sera comme à l'époque des bases de données soi-disant toutes au format SQL et où la compatibilité n'était en pratique que peu utile car elle ne concernait que la partie émergée de l'iceberg* », juge ainsi **Justin Ziegler**, le DSI de PriceMinister. Car, oui, encore une fois, le problème de l'interopérabilité n'est pas une caractéristique du Cloud public. Il existe depuis toujours.

Attention au respect de la législation

En France, la législation stipule, d'une part, que les informations à caractère personnel ne peuvent être transmises à d'autres personnes que celles à qui elles sont confiées par contrat et, d'autre part, que les personnes ou entreprises qui en ont la garde doivent avoir effectué certaines formalités (déclaration, demande d'autorisation…) auprès de la CNIL. Problème, dans le cas du Cloud public, et au prétexte d'offrir un service toujours disponible, **les informations sont dupliquées sur plusieurs centres de données** par le monde, y compris dans des zones géographiques qui n'ont que faire de la législation française, c'est-à-dire hors d'Europe. Ainsi, le droit français (comme celui de la plupart des pays européens) considère que les données d'un individu confiées à un tiers restent la propriété de cet individu et le tiers a le devoir d'en assurer la protection. En revanche, dans le droit anglo-saxon, le tiers est considéré propriétaire des données et n'est soumis à aucune obligation de protection. C'est ainsi que le gouvernement américain a pu consulter en toute légalité les données des utilisateurs de plusieurs fournisseurs de service en ligne. Pire, l'autorité américaine s'applique également en Europe, dès lors que les centres de données appartiennent à une entreprise américaine. De sorte qu'une offre de Cloud public utilisée pour héberger des coordonnées de clients, par exemple, n'est légale qu'à partir du moment où cette offre est 100% européenne, voire uniquement française et qu'elle s'est référencée auprès d'une CNIL européenne. Le cas des données de santé, qui ne peuvent être hébergées que chez un fournisseur de Cloud agréé, relève d'un décret particulier qui ne s'applique pas aux autres secteurs. Le fait que les banques ne stockent par leurs données dans des Cloud publics n'est ainsi dû à aucune législation, mais juste à la crainte des établissements bancaires d'exposer des informations sensibles.