La confiance numérique, une condition *sine qua non* du succès de l'adoption du *cloud*

Par **Marc DARMON**
Directeur général adjoint, Thales
Systèmes d'Information et de Communication sécurisés
et **Olivier KERMAGORET**
Directeur du Segment Services managés, Infrastructures critiques et *Cloud*

Le *Cloud Computing* est devenu, en l'espace d'une dizaine d'années, une véritable réalité économique et opérationnelle. Ainsi, selon le rapport « *Cloud* et Sécurité » (CXP, 2018), 40 % des infrastructures informatiques en France utilisent une architecture *Cloud*, un quart d'entre elles étant déployées dans une version publique. Pour autant, le *Cloud* reste encore un univers en fort développement, comme le montre une récente étude réalisée conjointement par Thales et Pierre Audoin Consultants qui fait état d'une croissance de 33 % en 2018. Ces différents types de *Cloud*, qu'ils soient publics, privés ou hybrides, ont désormais atteint un niveau de maturité suffisant pour nous permettre d'avoir du recul sur leurs avantages mais également d'apprécier les difficultés auxquelles il faut faire face lors d'un projet de migration d'une informatique dédiée vers un *Cloud* [1].

Le *Cloud*, un levier indispensable de la transformation numérique

Diminution des coûts, flexibilité, agilité, réduction du *time to market,* etc. De nombreux facteurs expliquent le succès du *Cloud*. Mais son atout majeur reste sans doute sa capacité à projeter l'entreprise dans l'automatisation de la production informatique de façon sécurisée (processus de type DevSecOps [2]), tout en proposant des services complets de type SaaS (*Software as a Service*) grâce auxquels les entreprises bénéficient de fonctions métiers mutualisées et à forte valeur ajoutée (CRM, outils et messageries collaboratifs, RH…). Le SaaS est devenu de fait le mode privilégié de consommation du *Cloud*, puisqu'il représenterait désormais 54 % du marché [3].

Par voie de conséquence, le *Cloud* est devenu un levier indispensable de la transformation numérique, au centre de la compétitivité des entreprises. Pour BPIfrance, une entreprise sur cinq est condamnée à disparaître si elle n'entame pas sa transformation d'ici trois ans. En effet, le *Cloud* est indispensable aux applications numériques, notamment lorsqu'elles s'appuient sur le *big data*, l'Internet des Objets ou l'intelligence artificielle, qui nécessitent des infrastructures hautement et instantanément évolutives. Il offre aussi la possibilité de tester ces nouvelles applications rapidement avec un investissement très faible.

La cybersécurité, le facteur « confiance » du *Cloud*

De ce fait, la cybersécurité du *Cloud* est un enjeu crucial, une impérative nécessité pour une transformation numérique réussie. Aujourd'hui, les chiffres parlent d'eux-mêmes : 95 % des failles

(1) « HySIO Flex : le cloud de Thales, Une expérience de dix ans riche d'enseignements ».
(2) De DevOps à DevSecOps, modèles de maturité.
(3) http://blog.markess.com/2018/07/tendances-cloud-computing-2020/

de sécurité dans le *Cloud* sont liées à son utilisation par les entreprises (déploiement d'architectures non sécurisées), 15 millions d'attaques sur les connexions ont eu lieu sur le premier semestre 2019 pour 400 000 réussies, 85 % des organisations ont été spécifiquement ciblées par des attaques et 45 % d'entre elles ont eu au moins un compte compromis dans le *Cloud*[4]. Le rapport de référence Symantec[5], basé sur les informations collectées par 123 millions de capteurs consignant chaque seconde des milliers d'incidents liés à des menaces dans cent cinquante-sept pays et territoires, fait état des grandes tendances suivantes :

- Les attaques de *formjacking* (ou piratage de formulaire) ont grimpé en flèche, avec en moyenne 4800 sites web compromis chaque mois.
- Les *ransomwares* délaissent les particuliers pour cibler les entreprises, dont les infections ont augmenté de 12 %.
- Plus de soixante-dix millions de fichiers ont été dérobés dans des compartiments S3 mal configurés, conséquence directe de l'adoption rapide du *Cloud*.
- Les chaînes logistiques restent des cibles faciles, avec une hausse de 78 % des attaques.
- Enceinte connectée, reine des cyberattaques : les appareils IoT constituent un point d'entrée majeur pour les attaques ciblées ; la plupart des appareils connectés sont vulnérables.

Malheureusement, la sécurisation des systèmes d'information est encore parfois perçue comme un coût, un mal nécessaire dont l'apport de valeur resterait à prouver. La cybersécurité est devenue, au gré d'attaques aux conséquences parfois dramatiques et de régulations toujours plus exigeantes, une condition *sine qua non* du succès des solutions numériques. Qui peut imaginer une voiture connectée et pilotée depuis un *Cloud* d'entreprise, vulnérable à n'importe quelle attaque ? La confiance que les utilisateurs portent à une solution numérique est un élément déterminant de son acceptation. Il n'y a pas de solution numérique sans confiance et il ne peut y avoir de confiance sans cybersécurité. En ce sens, la cybersécurité est devenue un différentiateur qui conditionne le succès de la transformation numérique. Gardons bien à l'esprit que les systèmes informatiques, désormais massivement interconnectés, sont attaqués en permanence. Plus les systèmes informatiques regorgent de données et de traitement, plus ils représentent un intérêt pour les attaquants, quelles que soient leurs motivations. La question n'est plus de savoir si ces systèmes seront attaqués un jour, mais quand et comment ils le seront, et quelle sera leur résilience.

On pourrait penser qu'il n'y a là rien de nouveau et que la cybersécurité dans le *Cloud* n'est jamais qu'un prolongement de la cybersécurité dans des environnements classiques. Certes, les familles de menaces sont les mêmes mais les caractéristiques du *Cloud* introduisent un changement de paradigme :

- La volatilité des ressources dans le *Cloud* rend nécessaire le déploiement automatique et instantané de dispositifs de cybersécurité (par exemple, la mise en place d'un outil de filtrage comme un *firewall*).
- Il est facile et rapide pour des utilisateurs de souscrire à des services *Cloud*, de développer et déployer des applications, mais les responsables sécurité ont besoin de garder la maîtrise de leurs systèmes et d'avoir une visibilité exhaustive et en temps réel des services utilisés.
- La surface d'attaque augmente, en particulier lorsque les services de *Cloud* sont accessibles directement *via* des adresses publiques.
- La responsabilité est partagée : une partie de la cybersécurité est assurée par le fournisseur de services de *Cloud*, alors que l'autre partie, souvent importante, reste sous la responsabilité de l'utilisateur. Il est impératif de maîtriser cette cartographie des responsabilités.

(4) https://www.proofpoint.com/us/threat-insight/post/cloud-attacks-prove-effective-across-industries-first-half-2019
(5) https://resource.elq.symantec.com/LP=6863?inid=symc_threat-report_istr_to_leadgen_form_LP-6863_ISTR-2019-report-main&cid=70138000001QvLeAAK

- L'utilisation du *Cloud* impose des processus et des outils spécifiques qui ne soient pas sous le contrôle de l'opérateur de *Cloud* et qui permettent de gérer la sécurité des données et des accès (chiffrements, gestion d'identité, gestion des clés…). Dans ce cadre, il est essentiel pour les entreprises de désigner un tiers de confiance capable de les accompagner dans le choix et la gestion de ces outils.
- La nécessaire « hyper-connectivité » pour accéder aux services *Cloud* peut ouvrir de nouvelles failles *via* les réseaux d'interconnexion et de nouvelles dépendances.

Multi-Clouds : une approche pragmatique

Il est maintenant clair que le marché s'oriente vers des solutions de *Cloud* hybrides, *multi-Clouds*, mixant *Clouds* privés et publics. La plupart des entreprises choisissent cette stratégie pour deux raisons simples : d'une part, la solution unique qui répond à tous les besoins n'existe pas, et, d'autre part, elle ne permet pas de prendre en compte le niveau de sensibilité des données et les contraintes de conformité associées.

Sur ces questions, le pragmatisme doit prévaloir. Des compromis sont nécessaires pour prendre en compte les enjeux et le rapport risque/bénéfice de chaque solution, avec quatre critères de décision : l'attrait du modèle d'affaire du *Cloud*, l'attrait de l'offre technique et fonctionnelle du *Cloud*, la dépendance à un fournisseur et la souveraineté des données.

Les deux premiers points figurent souvent parmi les préoccupations des organisations, même si les risques d'indisponibilités ne sont pas toujours identifiés. En effet, si les principaux fournisseurs de services de *Cloud* proposent des mécanismes pour assurer la disponibilité des applications, l'application elle-même doit être conçue pour mettre en œuvre ces mécanismes et s'intégrer dans les solutions de *Edge Computing* fournies par les opérateurs de *Cloud*. Par ailleurs, bien que les fournisseurs de *Cloud* public annoncent quelques niveaux de service (performance, disponibilité, temps de réaction et de résolution des incidents…), leur engagement est, dans les faits, très limité puisque les pénalités en cas de défaillance sont faibles voire nulles et les marges de négociation inexistantes. Les architectures doivent donc être conçues dans ce sens.

La deuxième grande question que doivent se poser les organisations en construisant leur feuille de route *Cloud* est la dépendance aux fournisseurs, le risque de *Vendor Lock-in*. Les plus grands *Clouds* publics offrent aujourd'hui un catalogue de services de haut niveau, les fameuses APIs, inégalées… et propriétaires ! Ces APIs sont un formidable accélérateur des nouveaux projets mais elles créent aussi une dépendance de fait avec un fournisseur. Avec leur utilisation, la réversibilité devient très théorique parce que très onéreuse. L'un des risques est la dépendance vis-à-vis d'acteurs qui modifient unilatéralement leurs grilles tarifaires ou leur modèle d'affaire. Ici, l'importance et la durée de vie du logiciel seront déterminantes. On n'aborde pas de la même manière un logiciel stratégique et un logiciel qui ne l'est pas, un logiciel d'utilisation temporaire et un logiciel qui durera plus de vingt ans.

Enfin, le dernier point, trop souvent sous-estimé par naïveté ou manque de sensibilisation, est certainement le plus crucial : il s'agit de celui de la souveraineté.

La souveraineté des données est entendue ici au sens du contrôle qu'une organisation, quelle qu'elle soit, doit avoir sur ses propres données. Il faut bien entendu penser souveraineté nationale, mais également souveraineté d'entreprise !

Traiter toutes les données de la même manière, avec un niveau de protection équivalent quelle que soit leur valeur ou leur sensibilité, n'a pas de sens. Un niveau de protection très important de toutes les données peut s'avérer contreproductif, car cela ne permettra pas à l'organisation concernée de bénéficier de tous les avantages du *Cloud*. À l'inverse, un niveau global de protection

faible fera peser bien trop de risques sur des données sensibles. L'analyse et le classement des données en fonction de leur sensibilité permettent donc de choisir des solutions de *Cloud* adaptées et de définir les justes mesures de protection. Ainsi, la richesse et la rapidité de mise en œuvre des solutions de *Cloud* publics sont séduisantes, mais elles peuvent être incompatibles avec le niveau de sensibilité de certaines données.

Les exemples de piratages massifs de données personnelles ou confidentielles sont quasi quotidiens car le *Cloud* offre, de fait, un large effet d'échelle en cas de vol de données. Des mesures de protection multiples peuvent permettre d'apporter une réponse globale efficace. Elles sont à la fois d'ordre organisationnel (définition et exécution d'une politique de sécurité, adoption de bonnes pratiques par les concepteurs, développeurs de solution, opérateurs en production, adoption d'une approche DevSecOps [6]) et d'ordre technique.

Parmi ces dernières, on peut citer en particulier le chiffrement systématique de toutes les données. Plusieurs solutions existent, par exemple VeraCrypt, orienté pour les besoins des particuliers, ou Vormetrics, que propose Thales à destination des entreprises. L'algorithme de chiffrement doit être suffisant pour résister aux attaques et les clés de chiffrement doivent être gérées dans une infrastructure de confiance indépendante du fournisseur de *Cloud*. Ainsi, le Chief Technology Officer de AWS, Werner Vogles, a indiqué, lors du AWS Summit de Berlin, en février 2019, la nécessité de ce chiffrement et d'une gestion indépendante des clés de chiffrement par la mise en place de solutions permettant le *Bring your own key* (BYOK). L'authentification des utilisateurs et la gestion de leurs droits doivent être assurées et l'activité tracée et supervisée de manière à détecter les tentatives d'accès non autorisées. Toutefois, le chiffrement des données n'est pas toujours possible, notamment dans les phases d'exploitation de ces données par des applications (modèle SaaS). L'anonymisation est une solution possible pour répondre en partie à ce défi.

Parmi les premières protections des environnements de Cloud figurent également la gestion d'identité et le contrôle d'accès (tel que le permet l'offre *Safenet Trusted Access*), afin de prévenir les risques d'intrusion. Ces mesures sont cruciales parce qu'elles sécurisent l'ensemble des environnements sur site et dans le *Cloud* et en particulier l'accès aux services, aux ressources et aux interfaces de programmation directement exposés sur Internet. Basées sur l'analyse des contextes d'utilisation, des populations d'utilisateurs ciblés, et de la sensibilité des applications auxquelles ces derniers accèdent, des politiques de sécurité *ad hoc* doivent être mises en place pour gérer le contrôle d'accès adapté, entre facilité pour l'utilisateur et niveau d'authentification nécessaire (telle que l'authentification forte multi-facteurs). La gestion des comptes à privilège doit être activée pour protéger les comptes d'administration, particulièrement sensibles du fait des droits étendus qui leur sont attribués.

Enfin, d'autres mesures techniques importantes s'appliquent à la protection des environnements de *Cloud*, comme les audits de code, les tests d'intrusion, les scans de vulnérabilité, la détection des menaces, les services de supervision de sécurité, etc.

L'impact du *Cloud Act* et des mesures à portée extraterritoriale

La question de la souveraineté des données dans le *Cloud* se double de risques supplémentaires liés aux lois extraterritoriales.

Le rapport établi par la commission d'enquête présidée par le député de Saône-et-Loire Raphaël Gauvin et intitulé « Rétablir la souveraineté de la France et de l'Europe et protéger nos entreprises

(6) De DevOps à DevSecOps, modèles de maturité.

des lois et mesures à portée extraterritoriale » débute par ce constat très inquiétant :

> « Les États-Unis d'Amérique ont entraîné le monde dans l'ère du protectionnisme judiciaire. Alors que la règle de droit a, de tout temps, servi d'instrument de régulation, elle est devenue aujourd'hui une arme de destruction dans la guerre économique que mènent les États-Unis contre le reste du monde, y compris contre leurs alliés traditionnels en Europe. (…) Les entreprises françaises ne disposent pas aujourd'hui des outils juridiques efficaces pour se défendre… »

Suit une liste non exhaustive d'entreprises non Américaines condamnées très lourdement par les États-Unis au motif que leurs pratiques commerciales ne respectaient pas le droit américain, alors même qu'aucune de ces pratiques n'avait de lien direct avec le territoire des États-Unis et/ou que ces entreprises se conformaient au droit de leur pays : BNP Paribas, HSBC, Commerzbank, Crédit Agricole, Standard Chartered, ING, Bank of Tokyo, Royal Bank of Scotland, Siemens, Alstom, Télia, BAE, Total, Crédit Suisse et demain, peut-être, Airbus, Areva, etc.

Selon le rapport, ces enquêtes et condamnations mettent en exergue cinq problèmes fondamentaux :

- Elles sont contestables et violent la souveraineté des pays.
- Les sanctions prononcées sont disproportionnées et menacent la pérennité des sociétés étrangères visées.
- Les enquêtes sont conduites sous le contrôle des procureurs américains, eux-mêmes placés sous l'autorité directe du pouvoir exécutif.
- Les conventions d'entraide judiciaire et les règles de la coopération administrative sont systématiquement contournées.
- Surtout, les poursuites engagées semblent être motivées économiquement et les cibles choisies à dessein.

Le *Cloud Act* semble s'inscrire pleinement dans cette stratégie, en imposant, dans certains cas, aux fournisseurs de *Cloud* public et aux opérateurs de réseau d'origine américaine l'obligation de fournir, à la demande des autorités judiciaires américaines, les données d'un client qu'ils gèrent ou qui transitent sur leurs réseaux, quelle que soit leur localisation géographique. Le fournisseur ou l'opérateur à qui une telle obligation est faite peut aussi se voir interdit d'en informer son client.

Les éléments de sécurité informatique que nous avons mentionnés ne permettent pas de répondre à ce problème. Des réponses peuvent être trouvées dans des solutions de *Clouds* privés ou publics offerts par des tiers de confiance européens, qui échappent donc au *Cloud Act*. C'est d'ailleurs pour cette raison que le Comité Stratégique de Filière de l'industrie de sécurité travaille, à la demande de Bruno Le Maire, ministre de l'Économie et des Finances, à la mise à disposition d'un ensemble des solutions de *Cloud* de confiance performantes, compétitives et indépendantes, en France voire en Europe.

Du *Cloud* civil vers la Défense et les armées

La transformation *Cloud* dans le monde civil a un impact pressant sur le secteur de la Défense. En effet, les utilisateurs, dans tous les rôles, vivent au quotidien les bénéfices du *Cloud*. Mais comme le pose le général Crall du *Department of Defense* américain : "Can it operate successfully in an information-contested environment, when a sophisticated adversary – *e.g.* Russia or China – is jamming your transmissions and hacking your network?" Le *Cloud* civil doit donc s'adapter à l'environnement militaire. Des prérequis supplémentaires et spécifiques s'appliquent à la Défense. La sécurité est très cadrée avec des référentiels comme celui de l'OTAN qui imposent une ségrégation étanche des flux et du stockage d'information suivant le niveau de confidentialité.

À cette sécurité exacerbée se conjugue l'impératif de souveraineté nationale, le risque émanant du plus faible maillon de toute la chaîne « sécurité et souveraineté ».

Ainsi, le modèle de déploiement en *Cloud* privé se détache comme solution pour les données classifiées et la projection sur les théâtres. Il garantit la souveraineté et l'adaptation aux conditions d'usage, tout en offrant les bénéfices du *Cloud* –décloisonnement des données, mutualisation des ressources, omni-disponibilité des services – en environnement contrôlé.

Le *Cloud* offre de formidables capacités de flexibilité qui transforment profondément l'informatique et par là-même nos organisations et la relation des entreprises avec leurs clients. Cette profonde mutation crée de nouvelles dépendances et peut se transformer en cauchemar économique pour les entreprises ou les administrations concernées, sans la mise en œuvre d'une véritable stratégie de mouvement vers le *Cloud* intégrant dès sa conception la dimension cybersécurité. Il ne s'agit pas d'injonctions contradictoires ou d'un mur infranchissable, car les solutions existent. Mais c'est une condition impérative pour établir une confiance durable et une vraie promesse de valeur.