

Les infrastructures au coeur de l'efficacité IT



En bref

C'est sans doute très à la mode de se préoccuper du digital. Bon. Mais il ne faudrait pas négliger l'essentiel, le concret, le solide, les fondations : les infrastructures. Ce sont ces infrastructures qui sont effectivement à la base de l'efficacité de l'IT. Numérique inclus.

Cela implique de réaliser des choix techniques souvent ambitieux. Parfois a priori risqués. Mais innover, avancer, suppose de gérer ces risques pour les maîtriser. Il n'y aurait en effet pas plus grand risque que de refuser d'avancer.

Sommaire

Technologies

Les infrastructures réseaux constituent le nerf de l'efficacité IT

Projets

L'Essec passe au stockage flash pour ses 1 200 postes de travail virtualisés

Projets

Comment le DSI d'Atkins migre 18 000 utilisateurs vers Office 365, version E5

Stratégie

La Société Générale s'expose pour se protéger et innover

Les infrastructures réseaux constituent le nerf de l'efficacité IT



Marie-Hélène Fagard (à gauche) a apporté son expertise durant l'atelier animé par Didier Barathon (à droite).

Le 20 septembre 2016 à Paris, CIO a organisé un Atelier Participatif sur le thème « Infrastructures réseaux : le nerf de l'efficacité - La performance et l'efficacité de l'infrastructure » avec Level 3, VMware et Intel.

L'infrastructure, c'est peut-être moins *glamour* que le digital mais ce dernier n'existe pas s'il ne repose pas sur des bases techniques solides. La performance et l'efficacité de l'infrastructure constituent en effet un fondement essentiel à la transformation numérique des entreprises. Mais comment les garantir ?

Pour répondre à cette question, CIO a organisé à Paris un Atelier Participatif le 20 septembre 2016 sur le thème « Infrastructures réseaux : le nerf de l'efficacité - La performance et l'efficacité de l'infrastructure » avec Level 3, VMware et Intel.

En s'appuyant sur un scénario fictif (voir encadré ci-dessous), la vingtaine de participants ont échangé autour de trois débats successifs : garantir la performance au meilleur coût, sécuriser les réseaux (avec Level 3) et virtualiser les réseaux (avec VMware).

Si Alain Khau (directeur commercial sécurité EMEA) et Christophe Belmont (ingénieur des ventes sécurité) pour Level 3 d'une part, Pierre Ardichvili (directeur des ventes réseau et sécurité Europe du sud) et Frédéric Grange (directeur technique réseau) pour VMware d'autre part ont apporté leur expertise lors de ces débats, Marie-Hélène Fagard, ancienne DSI de grandes entreprises (Europcar, Lagardère Active...) et actuellement consultante pour Fagard Associates et Mazard Advese, a su amener les participants à prendre du recul sur les thèmes abordés.

Disponibilité et sécurité

Les problématiques abordées ont donc été très larges : la disponibilité du réseau et sa performance pour de bons temps d'accès aux applications (notamment SaaS), les réseaux face à la mobilité des collaborateurs, la priorisation des flux, la complexité contractuelle, les coûts, les difficultés à bien gérer les droits d'accès et, bien entendu, la sécurité. Lors du tour de table initial, il a aussi été rappelé que la performance du réseau concernait bien entendu les collaborateurs mais aussi les clients. L'accès performant aux services fournis en ligne est essentiel pour la satisfaction de ceux qui entrent en contact commercial avec l'entreprise.

Les responsables IT présents ont mentionné deux difficultés souvent sous-estimées. D'une part, la réglementation pèse de plus en plus dans les préoccupations réseaux des entreprises. D'autre part, les entreprises intervenant sur les sites des clients héritent pour leurs propres agents des obligations des clients en matière de sécurité. L'exemple extrême cité est celui des intervenants BTP sur des sites de constructions de centrales nucléaires. Chefs de chantier et autres encadrant disposent évidemment d'un accès au réseau de l'entreprise comme à Internet, cumulant malgré tout les contraintes de l'industrie nucléaire avec celles de leur propre entreprise.

Le réseau est un point toujours critique

Un point particulièrement délicat est celui du M2M, notamment en cas de traitement intermédiaire dans le cloud. D'une manière générale, la connexion par des machines pose des soucis de sécurité et d'authentification. Deux exemples ont notamment été cités : d'une part celui des appareils médicaux en hôpitaux qui se connectent au dossier patient, d'autre part celui des compteurs *intelligents* tels que Linky. Ce dernier est actuellement déployé à raison d'un million d'exemplaires mais, à terme, ce sont 36 millions qui seront installés.

« Pour un manager IT de transition comme je peux l'être, le problème réseau est systématique lors de l'arrivée dans une entreprise et c'est un point critique depuis au moins quinze ans » a affirmé Marie-Hélène Fagard. Fiabilité, sécurité et performance constituent un triptyque de préoccupations incontournable. Pour Marie-Hélène Fagard, « avant, le réseau était moins crucial qu'aujourd'hui car les applications pouvaient vivre leur vie de manière isolée. Mais ce n'est bien sûr plus le cas aujourd'hui. »

Le SDN ne peut rien contre une pelleteuse (ou presque)

Pour répondre aux préoccupations évoquées, les tendances actuelles sont de miser sur l'agrégation de liens et la virtualisation des réseaux (SDN, *software defined network*). « Mais une pelleteuse qui casse physiquement le lien télécom lors de travaux sur la voie publique reste plus forte qu'un SDN » a relevé un participant. La rupture des liens physiques reste de fait le talon d'Achille de la virtualisation. Mais Marie-Hélène Fagard a exprimé son désaccord : « il est évident qu'on font deux pops utilisant deux routes pour éviter le problème de la pelleteuse » mais le SDN peut faire en sorte que ces deux infrastructures physiques soient gérées comme une seule infrastructure virtuelle. Bien entendu, l'hyper-convergence commence aussi à s'imposer dans le calendrier.

L'une des préoccupations exprimée est le besoin d'automatiser les différentes configurations réseaux (exploitation normale, exploitation de pointe, PRA, etc.). Trop souvent, les responsables réagissent face à un problème alors que les attentes des

utilisateurs, c'est une continuité de qualité, ce qui impose d'être prédictif pour anticiper les incidents. Enfin, le maintien de la qualité impose d'avoir un réseau physique dimensionné pour faire face aux pics d'activité, pas seulement à la moyenne d'utilisation.

Cybercriminalité et budgets : deux menaces sur les réseaux

De tels réseaux sur-dimensionnés par rapport à l'usage moyen ont évidemment un coût supérieur. Mais, pour Marie-Hélène Fagard, à l'heure du digital très exigeant en matière de réseau (notamment mobile), « les infrastructures ont retrouvé leurs lettres de noblesse alors que les budgets manquent. Le dialogue avec les métiers et le comité exécutif est essentiel pour définir les niveaux de service et les restrictions » en posant la question budgétaire clairement.

En plus des budgets, l'autre menace pesant sur les réseaux est bien sûr la cybercriminalité. A l'heure de la généralisation du cloud et de la mobilité, alors que les échanges entre entreprises sont au coeur de l'activité, « la prise en compte de la cybercriminalité va bien au delà d'un simple problème de virus sur un PC » a rappelé Marie-Hélène Fagard.

Sécuriser pour tous et partout

Opérateur télécom avec des infrastructures en propre (dont plus de 3500 kilomètres de fibres optiques), Level 3 a fait de la sécurité et de la fiabilité ses chevaux de bataille. « Il est difficile de prévoir un trafic réseau quand les métiers achètent leur SaaS dans leur coin, en shadow IT » a admis Christophe Belmont, ingénieur des ventes sécurité chez Level 3. Or l'infrastructure est évidemment fondamentale pour pouvoir se connecter à un cloud. La ressource en bande passante doit être utilisée par ceux qui en ont besoin mais le partage ne doit pas entraîner de complexité, ce qui constitue un défi difficile à relever.



Alain Khau (directeur commercial sécurité EMEA, à droite) et Christophe Belmont (ingénieur des ventes sécurité) chez Level 3.

Level 3 estime nécessaire que les entreprises mondiales disposent de points d'accès (*gateways*) sécurisés un peu partout dans le monde. Seule cette architecture, pour cet opérateur, permet aux travailleurs nomades ou localisés ailleurs qu'au siège d'accéder de façon sécurisée au SI de l'entreprise.

Le rôle d'un opérateur comme Level 3 est de sécuriser la liaison entre le terminal du collaborateur et le datacenter précis via un VPN. Ensuite, ce qui se passe dans le

datacenter, surtout si c'est celui d'un opérateur SaaS, n'est plus de son ressort. Pour garantir cette sécurité, Level 3 gère les 87 To de logs quotidiens du trafic sur son réseau propre en les traitant dans un cluster Hadoop afin de repérer les menaces. Il essaye ainsi notamment, autant que possible, de bloquer les adresses d'attaquants (notamment par DDOS) en bordure du réseau.

Permettre la révolution numérique

Une fois les attaquants bloqués, il n'en demeure pas moins que le responsable IT doit gérer au mieux les ressources physiques dont il dispose tout en garantissant agilité et fiabilité. « Nous avons déjà tous constaté les avantages de la virtualisation sur les serveurs ; l'idée est d'étendre ces bénéfices aux autres couches, notamment le réseau » a ainsi relevé Pierre Ardichvili, directeur des ventes réseau et sécurité Europe du sud chez VMware.



Pierre Ardichvili (directeur des ventes réseau et sécurité Europe du sud, à gauche) et Frédéric Grange (directeur technique réseau) chez VMware.

Bien entendu, ajouter une couche d'abstraction ne supprime pas la couche physique. Mais cela permet de rendre plus agile la gestion des ressources. VMware propose ainsi le Cloud Management Platform pour gérer les différents clouds, une solution de SDN et enfin Airwatch pour gérer les profils de terminaux se connectant aux réseaux. Rien de tout cela n'est une tendance pour un futur lointain : il s'agit bien du présent, par exemple avec 1400 grands comptes (EDF, Banque de France...) qui ont déjà déployé le SDN. Comme pour les serveurs, la virtualisation des réseaux permet d'en automatiser la gestion et d'accroître l'agilité de la réponse aux besoins métiers. Le coût d'exploitation des ressources physiques est ainsi nettement diminué. De plus, il est plus simple de changer l'infrastructure physique et cela facilite d'autant un PCA. Enfin, le SDN permet de créer des « bulles » totalement isolées. Pierre Ardichvili a ainsi mentionné l'exemple d'un office de la Défense Nationale qui « teste des virus dans une bulle en étant sûr de ne pas relâcher les malwares dans l'anature. »

Optimiser le trafic réseau interne au datacenter

La sécurisation passe aussi par la non-saturation des mécanismes de sécurité, y compris les mécanismes périmétriques. Or les transits entre serveurs au sein du datacenter passent souvent par les contrôles de cette sécurité périmétrique. Au point que le trafic serveur-à-serveur au sein d'un datacenter représente jusqu'à 80 voire 90 % du trafic local. Virtualiser la sécurité périmétrique permet de la démultiplier et de la rapprocher de chaque serveur, minimisant de ce fait le trafic interne au datacenter et

optimisant l'usage des ressources.

Enfin, le SDN permet de facilement déplacer des machines virtuelles d'une machine physique à une autre en emportant toutes ses méta-caractéristiques telles que l'adresse IP, les règles de sécurité, etc. , ce qui facilite d'autant l'administration du datacenter. Les migrations de ressources physiques peuvent ainsi s'effectuer en quelques minutes au lieu de plusieurs jours. Comme les réseaux gérés par SDN peuvent être totalement cryptés, cela permet à des entreprises d'utiliser des réseaux physiques de tiers sans risque. Par exemple, les données des pompes à kérosène des A380 d'Air France transitent via des réseaux d'aéroport mais avec une couche de virtualisation sécurisée.

Les budgets plus problématiques que la technique

« Pour assurer la sécurité, l'agilité, la redondance, nous avons toutes les techniques nécessaires » a constaté en conclusion Marie-Hélène Fagard. Mais il y a une grosse limite à l'usage de toutes ces merveilleuses technologies. C'est ce que Marie-Hélène Fagard a résumé aisément : « comment je fais pour déployer des solutions comme le SDN, afin d'accroître mon agilité et la sécurité de mon SI, tout en baissant les budget ? L'optimisation des coûts semble bien, une nouvelle fois, être la clé du reste.

Le scénario de l'Atelier Participatif

Comme support aux débats, les participants se sont appuyés sur un scénario fictif destiné à concentrer toutes les difficultés possibles. Bien entendu, il est souhaitable qu'aucune entreprise ne les cumule toutes.

« Léonce Déhaissy a des difficultés. La direction marketing a déployé sa nouvelle GRC en ayant recours à un SaaS mais le temps de réponse est très variable, selon la saturation du réseau. En particulier, quand la DAF récupère par FTP les données comptables des différentes filiales dans le monde, la performance réseau baisse pour l'accès à la GRC en SaaS. Les travailleurs nomades ont vu leur facture télécom exploser depuis le déploiement de l'app mobile de GRC qui se connecte à ce SaaS. Les services administratifs démentent formellement être à l'origine des difficultés même si chacun y connaît parfaitement les dernières webséries et clips à succès sur Youtube. Un pirate russe revendrait les données sur les clients de l'entreprise récupérées on ne sait trop comment mais visiblement il y a peu de temps. Enfin, Léonce Déhaissy est perdu entre tous ses liens internes, les droits d'usage des utilisateurs, comme dans ses contrats télécoms : le moindre paramétrage a un coût considérable et rien n'est jamais simple. »

Si tous les participants se sont accordés pour souhaiter ne jamais rencontrer toutes ces difficultés en même temps, deux aspects ont cependant été ajoutés en séance : les difficultés réglementaires et les contraintes budgétaires. De même, la relation clients a complété la relation utilisateurs internes.

[Retrouvez ici les documents associés à l'événement.](#)

Le prochain Atelier Participatif CIO aura lieu le 6 décembre 2016 sur le thème [Cybermenaces : savoir les affronter - Réagir avec pragmatisme et efficacité](#).



Bertrand Lemaire
Rédacteur en chef de CIO

L'Essec passe au stockage flash pour ses 1 200 postes de travail virtualisés



Olivier Le Mao est un adepte du VDI à l'Essec Business School

Pionnier du poste de travail virtualisé, l'Essec stocke désormais les données sur deux baies flash de Pure Storage.

« On a été parmi les premiers à faire du VDI il y a 7 ans. Nous avons adopté cette formule pour des raisons financières, en commençant avec Microsoft App-V (qui rend les applications disponibles aux utilisateurs sans qu'ils aient à les installer) et le client léger Neoware HP. Avant, les salles de cours étaient équipées de PC, avec des risques de vols ou de détérioration et une obsolescence des matériels. Professeurs et étudiants viennent maintenant avec leurs propres matériels, quels qu'ils soient, ils ont besoin de connexions rapides au poste de travail virtualisé.

Pour prendre en compte ces nouvelles demandes, il y a dix-huit mois, Olivier Le Mao, responsable systèmes à l'Essec Business School a opté pour un nouveau dispositif avec VmWare View 5.1 et des clients légers ThinApp en PCOIP (protocole d'affichage à distance pour les postes de travail virtualisés de VMware).

Sans appel d'offres, sur recommandation d'Antemeta

Le stockage s'effectue sur des baies PureStorage. « Moi, ce que je voulais, c'était la déduplication et la rapidité. Or, les disques durs étaient de vrais goulots d'étranglement. Sans appel d'offres, sur recommandation d'Antemeta, nous nous sommes intéressés aux baies Flash après être entrés en contact avec PureStorage. J'ai également observé leur mise en place chez Picard».

Les données de 1 200 postes virtualisés sont désormais stockées sur les baies de

PureStorage, deux baies pour une répartition de charge 50/50. Olivier Le Mao note plusieurs avantages : la réduction des temps de connexion dans les salles, en particulier après les pauses où les professeurs retrouvent instantanément leurs données, la réduction également de l'encombrement dans la salle machine du sous-sol de l'Ecole.



Didier Barathon
Journaliste

Comment le DSI d'Atkins migre 18 000 utilisateurs vers Office 365, version E5



Richard Cross regarde attentivement le réseau et la connectivité pour déployer Office 365

Le cabinet de conseil et d'ingénierie anglais Atkins, qui compte 180 bureaux dans le monde et 18 000 salariés, bascule sur Office 365.

Richard Cross, DSI D'Atkins, s'explique sur la migration de son entreprise vers Office 365. Cette décision s'intègre dans un plan global de migration, d'ici 2020, de tous les systèmes informatiques d'Atkins vers le cloud. Par rapport aux offres alternatives, le choix de Richard Cross a été relativement facile. « *Nous avons examiné Google Docs, mais notre familiarité avec les produits Office l'a emporté* », dit-il. « *Il y a aussi le fait qu'il fournit un espace de travail numérique, de sorte que nous pouvons avoir toute une gamme d'outils dans le cloud et y accéder à partir de tout terminal. Nous avons non seulement examiné l'aspect produit, mais surtout le fait d'avoir un espace numérique de travail dans le cloud.* »

Au mois de décembre dernier, Microsoft a lancé une version supérieure d'Office 365, nommée E5. Elle inclut tout ce qui était dans la version antérieure, la E3 : le courrier électronique hébergé, les applications bureautiques, Office Mobile et Skype for business. Mais E5 comprend également un PBX basé dans le cloud pour la téléphonie, des fonctions de sécurité supplémentaires et diverses options d'analyse qui ajoutent la visualisation de données aux capacités de recherche, propres à Office 365.

La migration a débuté et doit s'achever en 2017

E5 est destiné aux utilisateurs de type « power users » ceux qui ont besoin d'accéder rapidement à de l'analyse et ne sont pas basés dans leur bureau. Les salariés d'Atkins, ingénieurs et consultants, sont proches de ce profil. C'est pourquoi Richard Cross a

décidé de faire migrer toute la société, partout dans le monde, vers Office 365. « *Beaucoup de nos données sont encore stockées dans les bureaux locaux, mais nous avançons vers une version unique dans le cloud* ». La migration a débuté et doit s'achever en 2017, 10 000 personnes par exemple sont déjà sur Yammer, le réseau social d'entreprise intégré dans Office 365.

Richard Cross tire également les conclusions de sa migration et les précautions à prendre. De son expérience avec Microsoft, il a appris d'abord à bien négocier. « *Cela peut sembler évident, mais il faut être très clair sur ce qui est inclus dans Office 365 et ce qui ne l'est pas* ». Autre précaution, avec Office 365 il faut choisir un seul endroit pour être hébergé, « *ce qui signifie que vous devez regarder attentivement le réseau et la connectivité disponible partout où vous êtes implanté* ». D'autres, comme Berne Elliott du Gartner, estiment que la fonctionnalité PBX hébergé est encore immature et doit être provisoirement hébergée sur site.

Richard Cross conseille également à ses collègues DSI de veiller à ce que leurs besoins à long terme, 5 ou 6 ans, soient bien pris en compte par Microsoft. « *Nous avons envoyé une équipe à Redmond pour régler cet aspect* ».

Paul Rubens / IDG News Service (adapté par Didier Barathon)



IDG News Service

La Société Générale s'expose pour se protéger et innover



Carlos Goncalves, DSI de la Banque de Grande Clientèle et Solutions Investisseurs du groupe Société Générale, a présenté deux révolutions : la nouvelle architecture du SI et la mise en production continue.

En recréant son SI sous forme de briques ouvertes avec des API, la Société Générale protège son expertise tout en proposant plus de services.

« Il ne faut pas croire que la révolution numérique ne concerne que la banque de détail : il se passe aussi beaucoup de choses dans les autres métiers de la banque comme la banque privée ou les titres » a relevé Didier Valet, directeur de la Banque de Grande Clientèle et Solutions Investisseurs du groupe Société Générale. Il s'exprimait lors du rendez-vous Talk & Touch du 7 juillet 2016. Aux côtés de Alain Fischer, chief digital officer, et de Carlos Goncalves, DSI, il a présenté au cours de cette manifestation les évolutions considérables du SI de cette branche de la Société Générale autour du concept de *Digital Office*. Didier Valet a noté : « l'informatique est une part importante des frais généraux bancaires, entre 15 et 20% ».

Mais il a surtout insisté sur le fait que la révolution numérique ne se limite pas à ce que les clients voient, en gros les interfaces sur les systèmes publics « en tous lieux, à tous moments et sur n'importe quel appareil » (ATAWAD). Il y a, derrière, tout ce que les clients ne voient pas directement, même si, bien entendu, ils en bénéficient. Et cela concerne en particulier la flexibilité (grâce au cloud) et la sécurité.

Le *Digital Office* pour mener la révolution numérique

Pour mener la révolution numérique globale, la Société Générale a mis en place une cellule transverse dédiée baptisée *Digital Office*. Son objectif est à la fois de réaliser une veille technologique du marché pour repérer les innovations, de mettre en oeuvre la stratégie digitale du groupe, de superviser les projets, de communiquer pour faciliter la conduite du changement et enfin de promouvoir les *experts digitaux* au sein du groupe. Cette cellule est notamment animée par le CDO, Alain Fischer.

D'entrée de jeu, la Société Générale admet que le travail de refonte en cours est loin

d'être achevé. On en reparlera dans quatre à six ans. Il s'agit en effet de réaliser un reengineering complet du SI pour éliminer toutes les anciennes strates du legacy bancaire. Le chantier est donc particulièrement ambitieux. Et, au final, il s'agit bien de tout refondre avec une architecture basée sur de multiples briques interagissant via des API. L'objectif est d'atteindre une bien plus grande agilité avec le choix du *continuous delivery* mais pas seulement.

Les sept piliers de la sagesse digitale

Pour garantir la meilleure expérience au client, via les interfaces publiques ou grâce aux services mis en oeuvre, la Société Générale a défini sept piliers pour sa révolution numérique. Tout d'abord, exactement comme le Crédit Agricole avec son programme Nice (Nouvelle Informatique Communicante Evolutive), la Société Générale a choisi de développer des interfaces clients similaires aux interfaces utilisateurs internes, même si les droits d'usages restent différents et que, par conséquent, les fonctionnalités accessibles (via des onglets par exemple) resteront évidemment différentes. Cela amène -deuxième pilier- le choix d'une interface full web. « Le navigateur devient le poste de travail » a expliqué Alain Fischer.

Le point fondamental d'architecture est le troisième pilier : toutes les applications seront interconnectées et orientées services (API). Pour que les API soient utiles, il faut de ce fait appliquer des règles comme Google et ainsi passer d'une disponibilité, comme aujourd'hui, de 98% (même si tout le monde est content en interne) à un 99,99%. Evidemment -cinquième pilier- les indicateurs de mesure et d'analyse se doivent d'être pointus pour que le quatrième pilier soit effectif.

Grâce au troisième pilier, un sixième est possible : favoriser l'émergence d'idées innovantes. En effet, on peut s'appuyer sur les services existants via des API pour proposer de nouvelles offres de valeur. Alain Fischer a donné un exemple : « la banque a beaucoup d'informations sur les clients et leur en restituer un reporting peut en lui-même apporter de la valeur. Ainsi, pour des raisons réglementaires et de gestion, la banque calcule les taux de couverture de risques et leurs évolutions. Or, transmettre cette évolution de la couverture des risques à son client permet d'enchaîner un acte commercial pour accroître cette couverture. »



Alain Fischer, chief digital officer de la Banque de Grande Clientèle et Solutions Investisseurs du groupe Société Générale, a affirmé : « désormais notre expertise reste en interne et nous savons ce que le client utilise. »

Toutes les fonctions, à terme, sont destinées à devenir accessibles via des API et bénéficier d'un SSO. Ne pas connaître les API disponibles freine leur usage. Il s'agit donc bien d'exposer clairement ces API sur des portails de configuration automatique

pour multiplier les cas d'usages et donc les innovations en matière de services avec une facilité d'usage comparable à l'insertion d'un bouton Paypal sur un site web personnel. « L'interface utilisateur, c'est 5% du problème, le reste est la conception des briques et des API » a jugé Alain Fischer. De la même façon, la banque s'autorise à utiliser les API des FinTechs ouvertes pour enrichir ses services. Alain Fischer a observé : « quand le client d'Uber utilise Google Maps en encapsulation, il ne le voit pas et n'y porte aucun intérêt. »

Ce choix permet aussi de sécuriser le savoir-faire reconnu de la Société Générale. « Jusqu'à présent, nous envoyions des fichiers Excel à nos clients et partenaires, fichiers qui pouvaient arriver jusqu'à la concurrence alors qu'ils contenaient un savoir-faire au travers des macros et des formules ; désormais l'intelligence reste chez nous et on sait exactement ce qu'a fait notre client ou notre partenaire en utilisant l'API » s'est réjoui Alain Fischer.

Du cloud, oui, mais du cloud privé

De plus, les API permettent de facilement réutiliser les services disponibles. Carlos Goncalves a ajouté : « nous avons construit un démonstrateur avec Docker pour créer des conteneurs encapsulant des services afin de faciliter la réversibilité et l'indépendance vis-à-vis de nos fournisseurs d'infrastructure. » Pour l'instant, cependant, le recours à du cloud public reste une possibilité testée mais pas une réalité. Le cloud, à la Société Générale, est privé. « Et jamais nous ne mettrons des données clients dans le cloud public, ce sera juste du recours à de la puissance » a insisté le DSI.

Le cloud assure l'agilité d'infrastructure. Celle-ci vise, par exemple, à permettre d'absorber les pics de charge sur telle application à tel moment en ayant recours à de la puissance mise à disposition d'autres fonctions à d'autres moments. Pour le DSI, il s'agit d'être en mesure de provisionner ou de dé-provisionner des ressources aisément afin de garantir une parfaite élasticité des ressources face aux besoins à un instant *t*.

La mise en production banalisée

Côté développement, 60 à 70% sont aujourd'hui en mode agile. « En la matière, notre objectif est atteint » a indiqué Carlos Goncalves. Le véritable chantier actuel, pour accroître l'agilité, est le *continuous delivery*. Si les collaborateurs ont tous été formés à la méthode, c'est environ la moitié des développements qui utiliseront ce principe à la fin 2016. Les temps de mise à disposition d'un service nouveau ou modifié devront être au maximum de 2 à 4 semaines.

Le *continuous delivery* suppose une transformation à la fois IT et business. Il s'agit de faire du passage en production quelque chose d'anodin. Cela implique que tous les tests doivent être automatisés et rapides. Multiplier les mises en production permet de faire de petites mises en production régulières. Du coup, « la trajectoire peut être adaptée si les livraisons ne satisfont pas totalement le client final » a déduit Carlos Goncalves.

La guerre des talents

Pour atteindre tous ces objectifs, les ressources humaines constituent un véritable enjeu pour la Société Générale. Il s'agit en effet de disposer des « meilleurs talents ». Et le groupe embauche ainsi 200 à 250 ingénieurs par an dont une centaine de juniors. Pour accueillir ce personnel croissant, une technopole appartenant au groupe va être mise en place à Val de Fontenay. Le déménagement des équipes se déroulera de

septembre à décembre 2016 en abandonnant divers locaux loués un peu partout en Île-de-France.

Enfin, diverses innovations sont regardées par le groupe afin d'être prêt à les implémenter si cela devient pertinent ou possible. L'implémentation sera d'autant plus aisée si le SI est bien organisé en services exposés via des API. Typiquement, le Bitcoin et la Blockchain en font partie. « La blockchain repose sur trois technologies anciennes, la cryptographie asymétrique, la base de données distribuée et la gestion du consensus » a relevé Alain Fischer. Pour l'heure, la Société Générale mène des expérimentations pour voir les applications possibles de cette technologie. Mais le secteur bancaire est très réglementé et les cas d'usage, de ce fait, sont pour l'heure forcément très limités puisque l'existence d'une autorité centrale est en général obligatoire.



Bertrand Lemaire
Rédacteur en chef de CIO

Pour toute demande concernant CIO.focus :

contact-cio@it-news-info.com

Une publication de IT NEWS INFO : 40 bd Henri Sellier 92150 Suresnes

Rédacteur en chef : Bertrand Lemaire, blemaire@it-news-info.com

Tél. : 01 41 97 62 10

Principaux associés : Adthink Media et International Data Group Inc.

Président : Bertrand Gros

Directeur de publication : Bertrand Gros

Directeur général : Jean Royné

Président du groupe Adthink Media : Sylvain Morel

CIO est édité par IT NEWS INFO, SAS au capital de 3000000 €

Siret : 500034574 00029 RCS Nanterre

