Nouvelles technologies

Cloud computing : la sécurisation des données dématérialisées

Dans l'entreprise comme chez les prestataires, la culture de la sécurité s'enracine pour un passage serein vers le cloud

Peut-on se fier au cloud□? La peur liée au risque de perte de données lors du passage à la dématérialisation est-elle justifiée□? Ces inquiétudes, légitimes, sont l'un des freins qui ralentissent l'adoption du cloud par les entreprises. Pourtant la sécurisation des données est l'une des priorités des fournisseurs de solutions. Les techniques de protection sont aujourd'hui, quoique perfectibles, bien rodées et embarquées dans l'ensemble des gammes de solution. Par ailleurs, la forte implication des acteurs de la dématérialisation pour préconiser de bonnes pratiques réduit drastiquement les risques et permet au plus grand nombre d'envisager le cloud en toute tranquillité.

Le passage au cloud computing et à la dématérialisation des données est présenté comme la nouvelle bouffée d'oxygène des entreprises. C'est la promesse de la réduction des coûts administratifs, de la suppression de la plupart des tâches les plus pénibles et les moins gratifiantes… en somme, un ticket d'entrée dans le meilleur des mondes. Alors pourquoi aujourd'hui toutes les entreprises n'ont-elles pas encore franchi le cap□? Trois des cinq points les plus sensibles constituants un frein au cloud, selon une étude réalisée par Markess International auprès de 370 décideurs de PME, sont liés à la sécurisation, au sens large, des données. Alors si le cloud computing pourrait bien être la clé vers une meilleure gouvernance des données en entreprise, l'inquiétude demeure.

Quelle sécurité pour les données dématérialisées□? Les fournisseurs de solutions de dématérialisation intègrent-ils au mieux la question de la sécurité□? Toutes les possibilités de brèches ont-elles été envisagées afin de préserver de façon optimale les données confiées aux prestataires de solutions□? Par ailleurs, les entreprises qui se tournent vers les solutions de dématérialisation doivent-elles laisser la question de la sécurité à la seule responsabilité des fournisseurs de solutions□? Si la dématérialisation permet effectivement aux entreprises de faire des gains substantiels et aujourd'hui démontrés, les dirigeants doivent se saisir des questions qui les inquiètent afin de devenir partie prenante dans l'évolution de leurs pratiques.

L'analyse de risques, collaborative et évolutive
Craindre pour ses données est légitime. Mais encore faut-il savoir de quoi avoir peur pour

comprendre s'il y a des raisons de s'inquiéter. La dématérialisation concerne l'ensemble des services d'une entreprise, de sa comptabilité à ses données clients, de son flux d'activité quotidien à ses archives. Une entreprise peut aujourd'hui se retrouver mise sur serveur dans son intégralité. Il est en effet théoriquement possible qu'une entreprise se retrouve avec zéro papier et que tout ce qui la concerne, de son activité à ses preuves d'existence légale, soit numérisé dans des fichiers électroniques sur un serveur qui pourrait ne même pas lui appartenir.

Lorsque l'on pose le problème ainsi, il est facilement compréhensible que les dirigeants s'inquiètent de ce passage au tout numérique. C'est pourquoi il convient de définir les risques propres à la dématérialisation afin de pouvoir déterminer si les réponses apportées sont nécessaires et suffisantes ou pas. Ainsi, avant de se lancer dans un chantier de dématérialisation de l'entreprise, est-il nécessaire de procéder à une analyse de risques. "L'analyse de risques dépend de la maîtrise de cette analyse par l'entreprise, explique Pascal Antonini, président de l'Association française de l'audit et du conseil informatique (Afai) et associé chez Ernst & Young. Il est important d'y associer les parties prenantes, les compétences métiers. Car ce sont elles qui ont la connaissance de la sensibilité finale et intrinsèque des données. Sans cela, une analyse de risques ne tiendra pas la route. Si ensuite, on décide d'aller dans le cloud pour des raisons économiques, au moins y aura-t-il une connaissance assumée et comprise des risques encourus."

La Cnil (Commission nationale de l'informatique et des libertés) a rédigé et rendu publiques sur son site Internet des recommandations en direction des entreprises qui envisagent de souscrire des services de cloud. Elle identifie les principaux risques auxquels s'exposent les entreprises, que l'on peut diviser en deux registres. Le premier concerne les risques technologiques, et le second les risques liés à la prestation de service. Cette typologie permet aux entreprises qui souhaiteraient passer le cap de la dématérialisation de bien différencier ce qui dépend d'elles de ce qui relève de paramètres extérieurs.

En outre, les risques ne sont pas les mêmes en fonction des offres de cloud computing disponibles sur le marché. Les différents modèles de services, ainsi que les différents modes de déploiement proposés, n'auront pas les mêmes conséquences sur la gestion du risque. Choisir une solution de déploiement publique implique par exemple de partager les serveurs du prestataire avec d'autres clients. Or, malgré les efforts des prestataires de solution, ce modèle accroît les risques encourus par les données. Corinne Brizard, chef de produit dématérialisation Prologue, assure néanmoins que "la sécurisation n'est pas liée au prix de la solution. Le prix des solutions dépend de la simplicité des messages et de l'importance des flux d'information. Mais l'exigence de sécurisation est la même pour toutes les solutions proposées. Il y a des systèmes certifiés et normés. Il s'agit de rassurer les utilisateurs de ces solutions, qui sont très performantes et assez économiques. Le maître mot de la sécurité est de s'assurer qu'il n'y a pas de rupture, pas de brèche, pas d'altération du document". Ainsi le niveau et la qualité de la protection sont-ils comparables d'une offre à l'autre pour un type donné de solution cloud. D'un modèle de service à l'autre en revanche, les caractéristiques de la sécurisation varient, et c'est donc en rapport avec le niveau de protection identifié comme nécessaire, et les risques analysés, que devra s'opérer le choix de la solution.

La sécurisation des échanges

Pour comprendre de quels risques techniques on parle, il faut comprendre ce qu'est exactement la dématérialisation des données. Dématérialiser ses données signifie, pour une entreprise, dématérialiser les flux d'informations qui relient l'entreprise au monde extérieur,

et l'entreprise à elle-même. La dématérialisation concerne ainsi les flux d'informations qui étaient jusque-là exprimés sous format papier. C'est donc la dématérialisation des documents, mais aussi et surtout des échanges. Le risque est donc que ces échanges, confidentiels par définition, puissent être interceptés. Comment sécuriser technologiquement des échanges numériques ?

Corinne Brizard répond : "Dans un échange, il y a toujours un émetteur, un récepteur, un espace d'archivage de ces données dématérialisées et le transport de ces données. Il va falloir sécuriser ces quatre domaines afin de rassurer la chaîne. Au niveau de l'émetteur, les solutions vont chercher les données qui font l'objet d'un contrat de dématérialisation directement dans le système informatique de l'utilisateur, et vont les traduire en un message informatique. Cette information sera signée électroniquement pour garantir l'identité de l'émetteur du document. Au niveau du récepteur, il aura également une signature électronique qui décryptera la signature émise par l'émetteur. Une autre solution consiste à équiper l'émetteur et le récepteur de stations EDI [échange de données informatisé, ndlr] qui automatisent le processus et garantissent, là aussi, les origines des données transmises. Le troisième point à sécuriser concerne le transport des informations d'un bout à l'autre de la chaîne. De l'émetteur vers le récepteur sera utilisé un réseau sécurisé et crypté. Les stations EDI dialogueront sur du réseau sécurisé. Enfin, il sera question de la sécurisation de l'archivage. Lorsqu'une information sort de la station EDI ou du système d'information, il faut qu'elle puisse être versée de façon sécurisée dans la solution d'archivage. Il existe pour cela des solutions d'horodatage, de cryptage des informations, qui permettent d'assurer la sécurisation de bout en bout."

La procédure revient donc à crypter à chaque étape les informations, de manière à ce que seul les entités possédant la clef de cryptage puissent décoder les informations. La question demeure : quid de la puissance de cryptage ? "L'ensemble du processus d'archivage est normé, répond Corinne Brizard. C'est-à-dire que lorsque l'on parle d'archivage électronique ou de coffre-fort électronique, il y a des normes qui cadrent et valident les systèmes d'archivage. La réversibilité, la lisibilité dans le temps, toutes ces questions sont dorénavant intégrées dans les normes. L'objectif des solutions proposées aujourd'hui est clairement de garantir la pérennité de l'information dans le temps." Chambersign, créée en 2000 par les Chambres de commerce et d'industrie françaises, est une autorité de certification qui a ainsi placé la proximité client au cœur de son utilisation. Elle propose des certificats destinés à la téléprocédure, parmi lesquels un certificat utilisateur permettant de sécuriser les e-mails (signature, chiffrement) et de s'authentifier pour accéder au serveur.

La maîtrise contractuelle du risque

La seconde famille de risques déterminée par la Cnil regroupe l'ensemble des risques contractuels ou liés à une mauvaise gestion de la part des prestataires de solutions. Bien souvent, les directions opérationnelles ou générales contractent des solutions sans avoir au préalable effectué une analyse de risque, ou sans avoir consulté la DSI (parfois parce qu'elles n'en possèdent pas). Il est vrai que la majorité des prestataires s'attache à minimiser les risques et à sécuriser les données dématérialisées au maximum. Mais il arrive que de mauvaises surprises se produisent.

La sécurisation technique des échanges ne fait pas tout. Il faut également que les entreprises qui désirent passer au cloud s'engagent dans le processus. Car la sécurisation est à assimiler à un processus en constante amélioration et évolution. Pascal Antonini, président de Afai, revient sur ce point dans le guide intitulé "Cloud Computing et protection des données, guide

pratique à l'intention des directions générales et opérationnelles", publié par le Cigref, l'Afai et l'Ifaci (Institut français de l'audit et du contrôle internes). "Dans le guide, nous proposons une grille d'analyse qui permet de poser les vraies questions, explique-t-il. Intitulée "les objectifs de contrôle", elle permet de déterminer les contrôles qui peuvent être mis en place et l'importance que l'on doit attacher à un certain nombre de dispositifs. Il s'agit de vérifier que l'on a suffisamment de contrôle à différents niveaux sur le prestataire. On est dans une logique de vérification des dispositifs de sécurité proposés. Un certain nombre de clauses contractuelles peuvent aussi être proposées pour la signature de contrat de cloud. Notamment des clauses d'audit, qui imposent aux fournisseurs de solutions une procédure d'audit." Ces objectifs de contrôle semblent répondre directement aux recommandations de la Cnil. Le principe permettant de sécuriser ses rapports avec son prestataire est donc, selon Pascal Antonini, "de ne pas se laisser dicter des solutions de sécurité proposées par les fournisseurs, mais d'engager véritablement un dialogue pour pouvoir analyser si les solutions conviennent ou pas, et si elles ne conviennent pas – dans le cas notamment de données très sensibles –, de demander au fournisseur d'améliorer sa sécurité".

La sécurisation des données passe donc par une approche proactive de la part des entreprises qui souhaitent dématérialiser leurs données. Il ne s'agit pas de rester dans la passivité et de se satisfaire d'une relation traditionnelle client-prestataire. Puisque les entreprises mettent entre les mains de leur prestataire l'ensemble de leurs données vitales, elles ne peuvent pas s'en remettre à lui sans s'investir dans la relation et vérifier que tout est contrôlable et contrôlé.

Si la sécurité des données dématérialisées mêle tout à la fois des problématiques techniques, juridiques, opérationnelles et même, parfois, des craintes irrationnelles, ces inquiétudes ne sont pas fondées sur des problèmes insolubles, au contraire. Tous les acteurs et parties prenantes du monde du cloud computing s'attachent à les résoudre au mieux. La mise en lumière de ces questions est la première étape de leur résolution, car ce qui inquiète le plus, c'est l'apparente complexité de ces problèmes qui, parce que nouveaux, semblent incompréhensibles et donc impossibles à résoudre. Ouvrir le débat en interne est, par conséquent, la meilleure manière de maîtriser et de réduire le danger.

Denis Remy, directeur du salon Cloud computing world expo *
"Une véritable lame de fond de la dématérialisation"

Quels sont les enjeux du salon ?
Ce salon a été le précurseur des événements cloud en France, puisque la première édition a eu lieu en 2010. C'est l'événement de référence par rapport à sa spécificité, centrée sur les services IT à la demande. Le salon s'appuie sur la thématique data center. Ces solutions, ces offres, intéressent un certain nombre de DSI, de chefs de projets pour les grands comptes, mais également un grand nombre de patrons de TPE/PME qui souhaitent mettre en place rapidement des solutions d'accès à l'information. Ces services et infrastructures IT s'appuient sur un certain nombre d'hébergeurs qui seront là, sur un certain nombre de sociétés qui vont proposer des solutions pour concevoir, moderniser, rénover et optimiser les data center. On attend entre 4 000 et 5 000 visiteurs. Les grands leaders du cloud seront présents, aux côtés de nouveaux entrants, en particulier les deux porte-étendards du cloud souverain.

Quelles sont les grandes évolutions du secteur ?
Les offres cloud sont, depuis un an, réellement matures, et de plus en plus de sociétés les utilisent. En 2010, lorsque nous avons monté l'événement, le visitorat était orienté écosystème (SSII, intégrateurs, revendeurs). Ils étaient les premiers à vouloir savoir comment allait

évoluer leur corps de métier. C'étaient les consommateurs innovateurs. Aujourd'hui, la tendance est inverse, puisque les offres ont évolué. La question n'est plus "est-ce que l'on y va ou pas ?" la question est "quand est-ce qu'on y va ?" Il y a une véritable lame de fond de la dématérialisation. Des freins ralentissent néanmoins encore l'adoption par tous de cette technologie. Au niveau des grandes entreprises, la problématique est différente. Certaines sont déjà pourvues en termes d'infrastructure, ce qui est un frein à l'externalisation. Dès lors, la mutation se fera progressivement et en fonction des besoins de l'entreprise. Pour les petites et moyennes entreprises, la question de la location des ressources informatiques ne se pose pas, puisque la plupart n'ont pas les infrastructures nécessaires au passage à la dématérialisation.

Les solutions de cloud proposées aujourd'hui misent-elle ssuffisamment sur la sécurisation des données ?
L'une des tables rondes que nous organisons s'intitule : "Contractualiser pour le cloud, est-ce équivalent à un contrat d'externalisation ?" Cette question juridique est au cœur de la sécurité des données, puisqu'il s'agit de déterminer, au fond, les responsabilités juridiques liées à la dématérialisation. Par ailleurs, plus techniquement, la sécurisation est une question multiple. Il y a un aspect positif, car l'utilisation des données sur un serveur tiers équivaut à une redondance de la sauvegarde informatique. Néanmoins, il y a un aspect négatif aussi. Les données étant externalisées, certains domaines d'activité restent frileux quand à cette externalisation. Les fournisseurs de solutions doivent réussir à relever les défis de la sécurisation. L'intérêt de notre salon est qu'il pose les questions qui sont au cœur de ce secteur. La table ronde : "Premier retour d'expérience sur les problématiques sécuritaires du cloud public" reviendra justement sur ces questions.

**les 10 et 11 avril au CNIT, Paris la Défense*

Législation du lieu de stockage
La protection des données se heurte au Patriot Act

Les données étant l'expression dématérialisée des informations détenues par les entreprises, la question de leur lieu de stockage n'est pas innocente. En effet, à chaque pays ses propres lois, qui s'appliquent aux data centers présents sur son territoire. Savoir dans quels pays sont stockées les données de son entreprise, et quelles sont les lois sur la confidentialité qui s'appliquent, s'avère vital lorsqu'il s'agit d'archives juridiques, de données clients ou encore de prévisions stratégiques de l'entreprise.

Le Patriot Act, aux État Unis, permet par exemple à l'État fédéral de faire des requêtes de données à n'importe quel prestataire de cloud qui dépend légalement des lois américaines. Pire, par le biais de la juridiction extraterritoriale, le principe s'applique même aux propriétaires de data centers qui ne sont pas sur le sol américain, mais qui ont une succursale ou leur siège aux États-Unis. Face à cet épineux problème juridique, la France est en train de se doter d'un "cloud souverain" financé par des fonds publics. Mais il n'est actuellement qu'au stade embryonnaire et son avenir reste incertain. En effet, l'un des deux projets de cloud souverain est porté par Numergy, jeune société dont SFR est actionnaire, l'opérateur étant lui-même filiale de Vivendi… lequel tombe sous le coup du Patriot Act. Une structure capitalistique qui annulerait donc totalement la souveraineté présumée de Numergy.

Cette juridiction extraterritoriale pose de fait un véritable casse-tête juridique. D'autant que l'enjeu de la confidentialité et de la protection des données rejoint bien évidemment celui de la guerre économique que se livrent l'Europe et les États-Unis. Aux yeux de l'Europe, sous

couvert de cette loi, les États-Unis disposent d'un instrument de veille économique déloyal. À l'inverse, les États-Unis répliquent que cette attaque à l'encontre du Patriot Act permet à l'Europe de jouer la carte du protectionnisme contre les géants américains du cloud. Le débat fait actuellement rage, mais a néanmoins permis à la France de commencer à se constituer son cloud souverain.

Pourtant, il n'est pas garanti que ce concept puisse prétendre à un avenir brillant. En effet, comment contraindre une entreprise qui souhaite développer une stratégie de dématérialisation optimale à ne choisir des offres que dans un marché restreint et par définition moins concurrentiel que le marché réel, international ? Et s'il est possible d'imaginer qu'une entreprise ne conserve dans le cloud souverain que certaines données sensibles, et choisisse des offres plus intéressantes pour le reste de sa politique de dématérialisation, n'allons-nous pas voir se transformer le cloud souverain en un chantier coûteux et sous perfusion, qui ne servira au final qu'à protéger certaines données pendant que ses concurrents internationaux continueront de proposer des offres plus intéressantes ? La solution ne serait-elle pas de proposer une contre-attaque juridique incluant une juridiction extraterritoriale, laquelle est par ailleurs demandée par un certain nombre d'observateurs juridiques sur de tout autres chantiers ?

Big data dans les PME
Transformer la donnée brute en valeur ajoutée

Rappelons une évidence, le big data n'a d'intérêt que si des outils de traitement assez puissants permettent d'analyser ces masses de données et de transformer ces amas de fichiers en réponses à des questions. Le big data, littéralement "masse de données", ne peut s'appréhender que conjointement aux analytics, qui sont les outils permettant de le traiter. Une fois leur usage entré dans les habitudes, big data et analytics devraient changer radicalement la manière dont travaillent les PME.

Car la prise de décision dans une PME est généralement moins guidée par des procédures – comme dans une grande entreprise – que par l'instinct de son dirigeant. Mais il y a fort à parier que le couple big data-analytics va modifier en profondeur la capacité d'analyse de l'environnement, et donc l'interaction que les PME auront à l'avenir avec leur environnement. Pour Patrice Poiraud, responsable de l'initiative smarter analytics chez IBM France sur le dossier big data, "l'enjeu du big data et des analytics pour les PME sera d'être capable de traiter de grands volumes des variétés de données en temps réel. Presque toutes les PME concernées se sont dotées aujourd'hui d'un CRM [solution de gestion de la relation client, ndlr], cela n'est plus un signe distinctif de la concurrence. Ce qui permet de se démarquer aujourd'hui, c'est d'être capable d'analyser un grand volume de données afin de pouvoir en tirer le maximum d'enseignements".

Exemple de ces enseignements dans un usage purement commercial : la connaissance client. L'utilisation et l'analyse du maximum de données internes et externes autour des comportements clients donne une visibilité maximale sur leurs comportements futurs. Cela permet d'opérer des segmentations comportementales, qui amènent à des interactions beaucoup plus fines et proches de leurs habitudes. Les suggestions d'Amazon reposent sur ce type de traitement des big data. S'attachant à analyser intelligemment les consultations d'articles, l'outil de suggestion propose des produits au plus près des comportements d'achat des clients Amazon. L'analyse peut être si fine que ces traitements analytiques des données

clients sont l'objet de vives critiques de la part de certains groupes de défense des consommateurs, autour du principe du respect de la vie privée.

Il est cependant possible de tempérer cette critique en notant que la sollicitation publicitaire existe, et que ces outils ne permettent, au final, que de la spécifier au plus près des attentes des consommateurs ciblés. Ainsi, le volume publicitaire ne s'accroîtra pas, mais son objet se précisera. Cela dit, big data et analytics ne se réduisent pas au seul usage commercial. L'avancée technologique permise par cet outillage est en train de produire une véritable révolution qui reste encore à explorer en profondeur et dont les conséquences sur les PME sont bien plus vastes.

Par Shiran Ben Abderrazak