126

CIO.FOCUS

Octobre 2016

Data Protection - Sécuriser, stocker, sauvegarder les données

En bref

CIO a organisé une matinée stratégique sur le thème « Data Protection - Sécuriser, stocker, sauvegarder les données » le 11 octobre 2016. Experts et témoins se sont succédé pour présenter les meilleures pratiques pour protéger, stocker et gérer le patrimoine informationnel des entreprises.

Sommaire

La parole aux métiers

Le patrimoine informationnel sous la menace de risques à maîtriser

Président de la commission SI de l'AMRAE, François Beaume a présenté sur la Matinée Stratégique CIO « Data protection » du 11 octobre 2016 une approche des risques pesant sur les données.

François Beaume, président de la commission SI de l'AMRAE (Association pour le Management des Risques et des Assurances de l'Entreprise), est intervenu sur la Matinée Stratégique CIO « Data protection » du 11 octobre 2016.

La commission SI de l'AMRAE (Association pour le Management des Risques et des Assurances de l'Entreprise) réunit des gestionnaires de risques dans de grandes entreprises autour des sujets relatifs aux risques portant sur les systèmes d'informations ainsi que les outils IT dont les gestionnaires de risques peuvent avoir besoin pour remplir leurs missions, les SIGR (Systèmes d'information de Gestion des Risques). Son président, François Beaume, est intervenu sur la Matinée Stratégique CIO « Data protection » du 11 octobre 2016 à Paris : il a présenté à cette occasion l'approche méthodologique des risques concernant le patrimoine informationnel. L'AMRAE, association de référence du domaine, compte un millier de membres de 750 grandes organisations publiques et privées.

« De quoi parle-t-on lorsque l'on évoque le *patrimoine informationnel* ? » s'est interrogé pour commencer François Beaume. Avant d'étudier les risques portant sur quelque chose, il faut en effet préciser exactement de quoi on parle. Ce *patrimoine informationnel* correspond à « l'ensemble des données, protégées ou non, valorisables ou historiques, d'une personne physique ou morale ». Partie du patrimoine immatériel des entreprises, ce patrimoine informationnel a une valeur qui s'accroît. On y inclut par exemple les données clients, les brevets, les logiciels, les bases de données diverses... François Beaume a insisté : il faut « identifier précisément le patrimoine en question dans une entreprise donnée sera un préalable à une démarche de protection. »

Appréhender les risques avec méthode

En fonction des conditions de stockage et d'hébergement des données incluses dans ce patrimoine, les risques susceptibles d'en affecter l'intégrité jusqu'à, éventuellement, la destruction varient. Les mesures à prendre sont du coup différentes selon les situations. « Il faut mener des campagnes d'études pour identifier, évaluer et définir les moyens de gérer les risques » a décrit François Beaume.
Si toutes les entreprises ne disposent pas en interne de gestionnaires de risques (*risks managers*), cela ne fait pas obstacle à une approche par gestion des risques. François Beaume a en effet spécifié : « cela reste une démarche qui peut être mise en oeuvre par la seule volonté de la direction générale ou du management. C'est avant tout une question de méthode. »

Quatre étapes dans une méthodologie claire

Cette méthode repose sur quatre étapes principales. La première, bien entendu, est de poser un diagnostic des risques : quel patrimoine, quels risques, etc. Une fois cette première étape achevée, la deuxième peut alors être lancée : la maîtrise et la réduction des risques. A partir de là, le niveau de risques est diminué, avec une fréquence de survenue de leur réalisation minimisée. « C'est avec ce niveau de risques que l'entreprise va devoir vivre quotidiennement et c'est donc ce niveau de risques qu'elle va devoir financer » a constaté François Beaume.
Le financement des risques constitue la troisième étape de la méthode. Le risque est une probabilité de survenue d'un événement. Si cet événement se réalise, il va avoir des conséquences dommageables pour l'entreprise. Ce sont ces conséquences qui vont devoir être financièrement couvertes. François Beaume a alors posé la question majeure : « est-ce que l'entreprise est en mesure d'assumer seule sur ses fonds propres ces conséquences ou doit-elle partager ou transférer ce risque ? » Le partage-transfert de risque repose sur les assurances, dont les contrats doivent être étudiés et les couvertures rapprochées des risques identifiés, ce qui est en général confié au risk manager. Enfin, la dernière étape repose sur le constat que rien n'est statique, que tout évolue sans cesse « en particulier dans le domaine d'activité des DSI » comme l'a relevé François Beaume. Par conséquent, il sera nécessaire de réaliser régulièrement un suivi et un audit des risques et de leur couverture. De ce fait, la démarche est une boucle itérative. François Beaume a asséné : « ce que l'on vise dans cette démarche, c'est bien que l'entreprise soit résiliente et demeure performante pour atteindre les objectifs qu'elle s'est fixée. »

Des actions concrètes à mener en partenariat

Chaque étape, présentée ci-avant de manière très théorique, se décline bien entendu au travers d'une série d'actions concrètes. Par exemple, la phase de diagnostic repose sur une cartographie ou une analyse des risques au niveau d'un groupe, d'une entité, d'une activité ou même d'un projet. Cette démarche aboutit à un « panier de risques » et à un certain nombre de mesures possibles à prendre. La réduction des risques pourra s'effectuer soit en agissant sur la fréquence de survenance (prévention) soit en veillant à réduire l'impact lors de la réalisation d'un des risques (protection).
« Ce n'est pas nécessairement le risk manager qui dispose de l'expertise nécessaire pour définir précisément chaque risque, ni les gérer au quotidien, mais, par contre, il va animer le dialogue avec chaque métier impliqué » a admis François Beaume. Il va s'assurer que les bonnes méthodes sont mises en oeuvre, grâce à un dialogue très riche avec tous les métiers, notamment la DSI, la direction juridique et la DRH. Ensuite,

c'est lui qui va devoir mener l'arbitrage entre autofinancement et transfert à l'assurance ou bien gérer concrètement la crise liée à un sinistre, avec PCA, et l'analyse de ce qui s'est passé, comment l'incident a été géré et avec quels résultats. « Heureusement tous les sinistres ne donnent pas lieu à des crises mais tous sont intéressants pour nourrir l'expérience et donc la boucle d'interaction pour mieux gérer les risques » a expliqué François Beaume.

Briser les silos par le dialogue et la méthode

La transformation numérique des entreprises amène une modification substantielle de la structure des risques. Et elle amène les risks managers à intensifier le dialogue avec la DSI ou la Direction du Digital. Et chaque métier doit contribuer à l'analyse des risques en fonction des évolutions constatées dans sa pratique. Pour François Beaume, « le risk manager doit briser les silos dans l'entreprise en amenant un consensus sur une vision des risques et des actions à entreprendre via de la méthode et l'animation d'un dialogue. »
La méthode comporte évidemment des métriques qui vont être partagées et adaptées en fonction des évolutions constatées. Enfin, le risk manager doit amener chacun à une nouvelle culture d'entreprise où les risques sont pris en compte dès les phases amont. François Beaume a jugé : « il vaut mieux consacrer un peu de temps en amont d'une activité pour estimer ce qui peut se passer et bien le gérer. C'est l'équivalent du fait de regarder à droite et à gauche avant de traverser une rue. »
Et un point ne doit pas être négligé : bien gérer les risques -le cas échéant à l'aide d'assurances-, c'est aussi s'occuper de la responsabilité juridique des dirigeants, responsabilité qui pourrait être recherchée en cas de sinistre. « C'est particulièrement le cas en matière de données personnelles » a rappelé François Beaume. Et il s'est réjoui pour terminer : « bien gérer les risques, par son dialogue entre les fonctions et le décloisonnement qui en résulte, est aussi une source d'opportunités. »

En savoir plus

- Le site de l'AMRAE présente ses activités.
- Retrouvez les résultats de l'étude CIO *Comment préserver le capital data de l'entreprise ?*.
- Retrouvez les contenus associés à la *Matinée Stratégique Data Protection*.

Bertrand Lemaire
Rédacteur en chef de CIO

Stratégie

Associer le bon stockage avec le bon service

Franck Labat, à gauche, et Sylvain Gibassier, à droite, ont fait ressortir les questions d'accréditation et de règlementation

Franck Labat, directeur technique de la Fédération Française de Tennis (et donc du tournoi de Roland Garros) et Sylvain Gibassier, DSI de Saint-Germain-en-Laye, sont intervenus lors de Matinée Stratégique « Data protection » du 11 octobre 2016.

Deux DSI ont accepté de dévoiler une partie de leurs choix en matière de stockage : Franck Labat, directeur technique à la Fédération française de tennis (FFT) et Sylvain Gibassier, DSI de la ville de Saint-Germain-en-Laye.
Deux exemples totalement différents permettant de prendre la bonne mesure du sujet et qui se sont exprimés lors de la Matinée Stratégique CIO *Data Protection* du 11 octobre 2016.

A la FFT d'abord, quand on parle données, on parle essentiellement de droit d'accès, et sur quinze jours, ceux de Roland Garros. « En dehors de « Roland », explique avec humour Franck Labat, on fait du tennis ! La FFT est une association loi 1901, qui assure toute la monétisation de Roland Garros, mais gère aussi 1 000 sites en direct, ceux des ligues et des comités départementaux ».

Roland Garros est *le* grand rendez-vous de la FFT, non seulement en termes sportifs mais aussi pour l'aspect données. Plus précisément, celui des accréditations. La FFT, c'est une PME de 350 à 400 personnes, beaucoup en CDD donc avec des problématiques d'accès.

Pour Roland Garros, elle passe de 350 / 400 personnes à plus de 10 000 et ce ne sont pas les mêmes d'un tournoi à l'autre. Certains restent trois mois, d'autres une journée, de toute façon à un moment ou à un autre, elles ont un problème d'accès à toute ou partie du SI. Seuls les ramasseurs de balle n'ont pas besoin d'accéder au SI ! »

Une accréditation segmentée

L'accès est donc le sujet le plus important avec une plateforme dédiée pour plusieurs populations : les joueurs, leur staff technique, les médecins et tout le personnel médical, toute la partie restauration (numériquement les plus importants). Tout passe par l'accréditation qui varie suivant les populations, suivant les postes et les différents sites. C'est donc la segmentation de cette accréditation qui fait l'essentiel du travail de Franck Labat. « Les gens de la Fédération n'ont pas accès aux mêmes données que les personnels d'accueil pour les VIP, chacun a un rôle très précis, c'est une gestion des ressources par les profils et les gens sont rattachés à une direction métier ».

La plateforme capte les demandes d'accréditation, pour la partie sportive et pour la partie services. Ceux qui sont enregistrés le sont sous tutelle d'un référent métier, c'est donc une délégation très précise des rôles, « on sait toujours qui a demandé quoi et pour qui, on peut remonter pour savoir qui a donné l'accréditation. Mais, souvent c'est l'erreur humaine qui pose problème, ce n'est pas la bonne photo ou pas le bon nom. Le vigile est le dernier maillon, lui vérifie et rapproche l'accréditation de la personne qu'il a en face. Ensuite, à nous de gérer ! Si c'est la personne lambda ce n'est pas trop gênant, si c'est le coach de Nadal, évidemment c'est plus embêtant, donc il faut être très performant dans cette gestion. Et chez nous, tout est en local pour contrôler de manière parfaite ».

Pas de cloud, même souverain

A Saint-Germain-en-Laye, une collectivité territoriale de 40 000 habitants avec 700 agents, le principal problème dans la gestion des données c'est l'aspect règlementaire et celui du patrimoine. « Les besoins de stockage sont importants, souligne Sylvain Gibassier, le DSI, pour les services techniques et la gestion de nos 750 bâtiments, ou pour l'entretien des équipements. On avait un stockage existant en fin de vie, il avait plus de cinq ans. On a cherché un remplacement. On s'est posé la question du cloud. Un texte de la direction des archives (ministère de la culture) et du ministère de l'intérieur, nous oblige, si l'on veut faire du cloud, à faire du cloud souverain. Des juristes et le Syntec Numérique ont réagi, disant que si on voulait l'imposer dans nos appels d'offres ce n'était pas conforme à la législation sur les marchés publics. Donc, on est reparti sur une infrastructure interne. »

Changer de stockage est en fait une problématique de volumes et de mode de stockage. La ville de Saint-Germain-en-Laye s'est évidemment intéressé à la technologie flash, qui n'a pas été retenue car ne correspondant pas aux besoins de performances de la ville. Deuxième raison, la problématique de coûts a également fait pencher la balance au détriment du flash, la ville portant son choix sur des baies disques. Les articles de presse ne manquent pas sur les aspects budgétaires, avec la baisse des dotations de l'Etat, 75% sur deux ans.

Flash n'aime pas la clim

Autre argument contre le flash, la climatisation dans les deux salles serveurs, distantes de 3 km. Si la « clim » tombe en panne, c'est le coup de chaud, et là les technologies flash le prennent très mal. Une étude de Seagate l'a démontré.

La FFT est également réservé sur le cloud. Pour d'autres raisons. « Le cloud c'est génial pour faire du PCA ou du PRA, mais nous, si un incident se déclare au stade on

ne fait pas le tournoi, donc on a rien à faire d'un PRA ! On a du cloud mais pas pour l'infra évènementielle, on a deux salles serveurs, on utilise du métro cluster de chez NetApp pour avoir les deux salles entièrement redondées en pur PCA sur deux sites. On se protège d'un incident sur l'une des salles ».

Par ailleurs, en dehors de l'accréditation, la FFT compte une autre constante pour Roland Garros, le broadcast. Là, la fédération passe par une baie flash pour la 4K, l'audio et toutes les données nécessaires pour envoyer aux chaînes du monde entier ce qu'a tourné France Télévision. La FFT a également proposé cette année un nouveau service digital, pour les joueurs, avec la disponibilité de leur match en vidéo, un quart d'heure seulement après la fin de l'épreuve. Et directement accessible par leur compte, avant c'était beaucoup plus long et sur une clé USB !

Sur le même sujet

- Retrouvez les résultats de l'étude CIO *Comment préserver le capital data de l'entreprise ?*.
- Retrouvez les contenus associés à la *Matinée Stratégique Data Protection*.

Didier Barathon
Journaliste

Technologies

Comment adapter sa politique de stockage ?

De gauche à droite : Christophe Puzenat de Solvay, Henri Codron, du Clusif, Philippe Martinez, du Synchroton Soleil lors de la table-ronde CIO

Henri Codron, du Clusif, Philippe Martinez, du Synchrotron Soleil et Christophe Puzenat de Solvay sont intervenus lors de Matinée Stratégique CIO « Data protection » du 11 octobre 2016.

Les stratégies de protection des données s'inscrivent-elles toujours dans la transformation des entreprises, en particulier dans leur évolution vers le cloud computing ? Comment a évolué la protection des serveurs et des applications à architecture Cloud ? Comment répondre aux nécessités en termes de continuité des opérations et de disponibilité des données ?

A ces questions répondaient les trois intervenants de la deuxième table-ronde, réunie lors de la Matinée Stratégique sur la Data Protection le 11 octobre dernier : Henri Codron, vice-président du Clusif, responsable de son Espace RSSI, Philippe Martinez, project manager, au Synchrotron Soleil et Christophe Puzenat, responsable de l'infrastructure delivery chez Solvay. Ce dernier étant, par ailleurs, le Grand Témoin, de la matinée.

Comme il s'occupe de l'Espace RSSI, regroupant 130 responsables en sécurité, membres du Clusif, Henri Codron, sait répondre aux problématiques de stockage définies en fonction de la sensibilité des données. « Nous avons constaté au sein du Clusif, remarque-t-il, le choix fait il y a 5 ou 10ans de stocker à l'intérieur de l'entreprise, dans le château fort comme on le disait. Nous sommes sortis de ce modèle, la DSI n'est plus seule à prendre la décision. Aujourd'hui, l'éparpillement des données est évident, soit en interne, soit dans le cloud qui se démocratise et change le paysage. Des migrations vers un cloud de type Office 365 ou Gmail, ouvre vers d'autre formes d'hébergement dans le cloud, par exemple avec le collaboratif ».

S'assurer de stocker au bon endroit et de la bonne manière

Cet éparpillement et le fait que les utilisateurs souhaitent accéder de partout, à partir d'un poste de travail, d'un smartphone, d'une tablette, oblige le responsable sécurité à proposer partout la même sécurité, donc à avoir un projet de classification des données en plusieurs chapitres, qui sont indispensables à l'accompagnement du projet cloud. De toute façon, il faut aussi, conseille Henri Codron, veiller à l'aspect accompagnement des utilisateurs. Le stockage et la protection des données ne doit pas rester l'affaire des seuls informaticiens, mais mobiliser les métiers dans la partie identification et sur la bonne identification. Il faut s'assurer de stocker au bon endroit et de la bonne manière. Et que les utilisateurs disposent du bon support. Quels sont les choix en matière de disque ou de bande ? Ont-ils une importance pour la protection des données. Pas pour le représentant du Clusif, « on ne parle pas de dispositif en particulier ».

Au Synchrotron Soleil, l'approche est très différente, nous sommes là dans un centre scientifique. On travaille avec de très grands instruments de recherche pour faire de l'analyse de la matière et de la structure atomique ou moléculaire. « On travaille aussi avec des industriels ouvert à tout type d'expérience » remarque Philippe Martinez, project manager. « Mais ce qu'il faut retenir, c'est que nous produisons beaucoup de données très hétérogènes, de quelques gigaoctets à plusieurs teras par jour ! Ensuite, nous devons arriver à rendre ces données disponibles. Or, ce sont des données scientifiques, peu compressibles, uniques, avec des formats et des tailles de fichiers très différents ».

Stocker la donnée et la rendre accessible

Le problème au Synchrotron est multiple, stocker la donnée, la rendre accessible, alors qu'elle arrive en masse, et en plus sur un certain nombre de points de collecte. « On a mis en place une architecture logicielle, avec Active Circle, une société créée par le fondateur d'Atempo. Elle donne la possibilité de distribuer les données ».

Autre élément important pour les intervenants, la pression règlementaire très forte avec GDPR qui demande, pour rester conforme de démarrer des projets de classification de données performants. Chez Solvay, on gère au plan mondial ce type de contraintes, par exemple GDPR qui est européen, mais aussi la Loi de programmation militaire (LPM) qui arrive en France avec les règlementations de l'ANSSI. Les Etats-Unis ont une règlementation qui protège les armements, du coup, elle suscite beaucoup de règlementations locales et atteint tout secteur pouvant contribuer de près ou de loin à l'armement.

Autre exemple, si vous allez dans le cloud, vous faites face à une règlementation aux Etats-Unis, une autre en France. Solvay dispose d'un réseau Wan d'entreprise distribué dans le monde entier. Et soumis à différentes règlementations locales. « On peut tout mettre dans le cloud, mais on ne peut pas faire marche arrière à cause des règlementations » souligne Christophe Puzenat, Infrastructure delivery manager France.

Didier Barathon
Journaliste

Projets

Préserver des données sensibles mais volumineuses

Christophe Puzenat, France Delivery Manager de Solvay, a été le Grand Témoin de la Matinée Stratégique CIO « Data protection » du 11 octobre 2016.

Christophe Puzenat, France Delivery Manager de Solvay, a été le Grand Témoin de la Matinée Stratégique CIO « Data protection » du 11 octobre 2016.

Solvay fait partie des plus grands groupes de chimie dans le monde avec plus de 32000 collaborateurs, 13 milliard d'euros de chiffre d'affaires en 2015, 31 centres de recherche et 145 sites dans 53 pays. Parmi ses activités de pointe, Solvay a une action forte dans les matériaux légers comme la fibre de carbone. « Solvay veut être le poids lourd de l'allègement » a indiqué Christophe Puzenat, France Delivery Manager de Solvay. Celui-ci a été le Grand Témoin de la Matinée Stratégique CIO « Data protection » du 11 octobre 2016 à Paris.

Chez un chimiste, les données à traiter sont très souvent de la plus haute importance pour ne pas dire au coeur de l'activité. Cela commence avec le HPC (calcul haute performance). « Avant d'acheter un produit, certains clients demandent à faire des simulations du comportement de celui-ci et cela nous impose donc de nous équiper en interne de moyens HPC » a ainsi précisé Christophe Puzenat. La vente de matière est en effet souvent lié à la simulation du comportement de celle-ci dans un contexte client déterminé. Et Solvay commercialise ainsi du service associé à ses matières, notamment dans les plastiques de spécialité utilisés en allègement de structures.

Sécurité, confidentialité, performance

A ces données HPC s'ajoutent des données issues des PC de laboratoires qui gèrent les données de recherche. Christophe Puzenat a pointé : « ce sont là des données temps réel, y compris de l'IoT lorsque l'on remonte de l'information de capteurs. » Les données issues de systèmes industriels MES (Manufacturing execution system) sont à la fois temps réel, très volumineuses et à garder parfois une quinzaine d'années. Evidemment, comme toutes les entreprises, Solvay doit aussi gérer les données

banales de son ERP et de ses systèmes supports. Sur ce dernier point, le chimiste n'a aucune particularité notable.
Solvay a donc des préoccupations non seulement de sécurité et de confidentialité -très classiques- mais aussi de pure performance lorsque l'on parle de HPC dans un contexte de données variées et volumineuses voire véloces (temps réel) donc de Big Data à haute performance. « Le stockage est choisi en fonction de plusieurs critères, le premier étant le volume de données concerné pour chaque type, le volume allant de modeste à intéressant » a noté Christophe Puzenat. Il a ajouté : « le deuxième est la performance d'accès -ce qui peut écarter d'entrée de jeu des solutions de type cloud-, ensuite la nécessité de garder en ligne les données sur une longue période immédiatement accessibles aux ingénieurs afin de pouvoir retravailler sur des algorithmes ou des expériences. Cela implique de ne pas recourir à des bandes abandonnées dans une armoire. » Pour tout cela, le système de stockage a été rénové en 2015.

Des performances et de la disponibilité à la demande

Solvay a lancé un appel d'offres auquel beaucoup de candidats ont répondu. Ce sont finalement les produits Infinibox d'Infinidat qui ont été choisis. La performance aussi bien pour le MES, le HPC et les données de laboratoire a été le premier facteur de séduction. Mais Christophe Puzenat cite également un autre plus produit : « le *storage on demand* au sens où le déblocage de capacités sur les baies installées se fait via une clé de licence obtenue avec un bon de commande, c'est donc très simple sans arrêt de production ou intervention de technicien. » 20 To, 40 To, 100 To peuvent ainsi être débloqués. Il est vrai que 330 To avaient été livrés pour 100 achetés au départ sur chaque baie (une de production, l'autre de backup, sur deux sites distants). « On est en actif-passif car on peut supporter un petit arrêt mais, par contre, il est inacceptable pour nous de perdre de la donnée » a spécifié Christophe Puzenat.
Les baies sont de technologie SDS avec des transferts de données au delà des espérances de Solvay lors de l'appel d'offres puisqu'on peut atteindre les 400 000 i/o par seconde. La virtualisation des disques est gérée sous VMware et la sauvegarde par la solution Veeam. Au final, tout est aussi sauvegardé sur bandes par mesure de précaution mais uniquement comme ultime étape du « ceinture, bretelles, parapluies » car, comme l'a dit Christophe Puzenat, « toutes données en ligne sont dans l'absolu piratables ou cryptables ».

Le cloud, pas n'importe lequel, pas pour n'importe quoi

Solvay dispose donc de pratiquement toute la panoplie de technologies disponibles : bandes, disques SATA, SDS... et du cache en RAM (400 Go !). Le cache SSD en plus, disponible chez Infinidat, a semblé une « cerise sur le gâteau pour du HPC à raison de plusieurs clusters sur une même baie. » Ce luxe n'a donc pas été choisi.
La confidentialité des données amène à demander des audits et des certifications poussés à des fournisseurs de cloud pouvant éventuellement un jour être éligibles à recevoir des données où la performance ne serait pas avec de hauts niveaux d'exigence. « Mais Solvay a toute sa messagerie chez Google, avec qui nous avons obtenu le respect de nos exigences » a rappelé Christophe Puzenat. Toutes les informations, tant de Solvay que de ses clients, font l'objet d'une analyse précise du niveau de risque et d'une classification. En fonction de celle-ci, ces données pourront ou pas être poussées sur le cloud. Le cryptage est exigé dans le cloud public. Pour éviter les dérives, certains services en ligne qui pourraient faire l'objet d'un recours en shadow IT (comme Dropbox) sont bloqués par les firewalls. Des systèmes de type DLP sont très coûteux et les services de stockage en ligne sont innombrables. Mais comme il

est difficile de tout bloquer, Christophe Puzenat a insisté : « il faut éduquer les utilisateurs pour éviter de se retrouver avec des données scientifiques un peu partout. » Certaines catégories de personnes ont des postes cryptés et une interdiction d'usage de supports de type clé USB.

Bertrand Lemaire
Rédacteur en chef de CIO

Business

Data Protection : sécuriser, stocker, sauvegarder les données

La Matinée Stratégique « Data Protection : Sécuriser, stocker, sauvegarder les données » a été organisée par CIO le 11 octobre 2016.

Le 11 octobre 2016, CIO a organisé à Paris une Matinée Stratégique sur le thème « Data Protection : sécuriser, stocker, sauvegarder les données » en partenariat avec ASG Atempo, Commvault, Google Cloud, HPE, IBM et Veeam.

Les entreprises sont-elles conscientes que la préservation de leurs patrimoines informationnels est absolument fondamentale à leur survie ? En ouverture à la Matinée Stratégique « Data Protection : Sécuriser, stocker, sauvegarder les données » organisée par CIO le 11 octobre 2016 à Paris en partenariat avec ASG Atempo, Commvault, Google Cloud, HPE, IBM et Veeam, la rédaction a révélé les résultats de l'enquête *Comment préserver le capital data de l'entreprise ?*. Et ceux-ci confirment que les bonnes pratiques sont loin d'être unanimement suivies.
Au cours de la Matinée Stratégique, bien au contraire, ce sont les meilleurs exemples et les bonnes pratiques qui ont été rappelés. Experts et témoins se sont ainsi succédés à cette fin.

Disponibilité, accessibilité et partage

« Aujourd'hui, la transformation numérique impose que les données soient disponibles, accessibles et partageables à tout moment » a alors martelé Gabriele Carzaniga, Sales Engineer Manager chez Google. Pour lui, cela impose de passer par un stockage dans le cloud. En choisissant un stockage chez Google, les données sont répliquées sept fois à travers le monde dans des datacenters reliés par un réseau de fibre optique dédié contrôlé par Google. La maîtrise est donc totale. La sécurité architecturale est, de plus associée à une sécurité contractuelle et à des engagements clairs de Google. En particulier, selon Gabriele Carzaniga, la localisation des données est un sujet moins

politico-juridique que purement technique, pour traiter la latence et donc la qualité de service.

Gabriele Carzaniga, Sales Engineer Manager chez Google, a détaillé comment assurer la sécurité et la conformité de vos données dans le Cloud.

Les risques pesant sur le patrimoine informationnel ont ensuite été étudiés par un expert de la gestion des risques, François Beaume, administrateur de l'AMRAE, président de la commission SI de l'AMRAE. Cette association regroupe des responsables de la gestion des risques et des assurances, comme son nom l'indique, Association pour le Management des Risques et des Assurances de l'Entreprise. Il a d'abord défini le patrimoine informationnel avant d'y appliquer la méthodologie de la maîtrise des risques et d'en tirer une démarche pragmatique. « En tant que gestionnaires de risques, je travaille avec différents métiers, notamment le DSI, en apportant de la méthode » a ainsi expliqué François Beaume.

Les risques pesant sur le patrimoine informationnel ont été étudiés par François Beaume, administrateur et président de la commission SI de l'AMRAE

Un capital à protéger

Philippe Decherat, Directeur Technique de Commvault, a d'ailleurs rappelé : « les données constituent un capital au même titre que la finance, le mobilier et l'immobilier. » Ce patrimoine doit évidemment être sauvegardé mais pour éviter un coût trop élevé tout en garantissant la préservation des données, Philippe Decherat a plaidé pour une hiérarchisation des sauvegardes. Un système de snapshots rapides permet ainsi d'optimiser les coûts par rapport à des backup traditionnels qui peuvent ainsi être moins

fréquents. Bien entendu, une solution unique permet de traiter plus efficacement l'ensemble des types de sauvegarde.

Philippe Decherat, Directeur Technique de Commvault Data Platform, a défendu sa position d'avant-garde de la sauvegarde restauration, dans le cloud ou pour toute infrastructure.

La maîtrise des risques sur les données était aussi le sujet de la première table ronde réunissant Franck Labat, Directeur Technique de la Fédération Française de Tennis (FFT), et Sylvain Gibassier, DSI de St Germain-en-Laye. Deux types de préoccupations ont ainsi pu être abordés : la gestion des droits d'accès avec du personnel très variable et l'archivage dans un contexte réglementaire contraignant.

De gauche à droite : Franck Labat (Directeur Technique de la Fédération Française de Tennis) et Sylvain Gibassier (DSI de St Germain-en-Laye).

Pour une politique de stockage garantissant la performance

« Il vaut mieux parler de Data Rétention, en centrant le débat sur le stockage et l'archivage, plutôt que sur la Data Protection, trop orientée sur la seule sécurité » a plaidé Stéphane Coche, Directeur Adjoint de la Division Stockage & Sauvegarde d'IBM Systems France. La politique de stockage doit en effet répondre à des problématique au delà de la seule sécurité périmétrique, à commencer, donc, par la performance. Mais le coût est aussi, bien sûr, le nerf de la guerre. De ce fait, il ne faut pas écarter par principe la bande magnétique qui reste le moyen de stockage le plus économique, mais savoir adopter les meilleures technologies dans chaque cas, en allant bien sûr chercher le stockage flash ou le stockage objet lorsque c'est pertinent. Et disposer d'une

approche globale, matérielle et logicielle, couvrant tout le spectre du stockage simplifie bien sûr la vie de l'entreprise.

Stéphane Coche, Directeur Adjoint, Division Stockage & Sauvegarde chez IBM Systems France, s'est inquiété de la protection des données à l'ère Schengen.

Une solution unique optimise les coûts

Serge Hardoin, consultant avant-vente chez HPE Software IM&G, a souligné : « une solution qui permet de tout faire optimise les coûts de personnel et de support ». Cette solution unique pour gérer le stockage, la sauvegarde et l'archivage, y compris dans le cloud, doit aussi être capable de suivre tout le cycle de vie de la donnée, jusqu'à sa destruction lorsque c'est nécessaire, par exemple pour respecter le droit à l'oubli. Mais la sauvegarde a parfois des applications connexes : par exemple, celle des postes de travail, s'il est bien menée, permet de lutter contre les ransomwares en remontant une version antérieure à la contamination de l'environnement de travail.

Serge Hardoin, consultant avant-vente chez HPE Software IM&G, a prescrit : « prenez le contrôle de vos données ».

Le Grand Témoin de la Matinée Stratégique a été Christophe Puzenat, France Delivery Manager de Solvay, qui a explicité quelles stratégies étaient mises en oeuvre chez ce grand de la chimie pour garantir la disponibilité et la protection de ses données.

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