« Cloud computing » et marchés publics : garantir la confidentialité

« Cloud computing » et marchés publics : garantir la confidentialité

L'« informatique en nuage » ou « cloud computing » permet à la personne publique de s'affranchir des contraintes liées à une infrastructure informatique complexe, et aux services publics de gagner en efficacité. Son utilisation pose cependant des questions sur la sécurité et sur la gestion des données transmises et stockées dans le cloud, qui est l'origine des normes mises en place depuis trois ans, fort utiles aux acheteurs publics.

Une analyse juridique de Nicolas Nahmias et Emmanuelle Bénoit, avocats à la cour, cabinet AdDen avocats

Le « cloud computing » ou « informatique en nuage » désigne le stockage de données (telles que des fichiers de texte, des images et des vidéos) et de logiciels, auxquels les utilisateurs accèdent par internet en utilisant l'appareil de leur choix.

Selon la Commission nationale de l'informatique et des libertés (Cnil), il s'agit de la forme la plus évoluée d'externalisation, dans laquelle le client ou l'utilisateur dispose d'un service en ligne dont l'administration et la gestion opérationnelle sont effectuées par un sous-traitant (entendu comme celui qui traite les informations personnelles pour le compte du responsable de traitement, selon ses instructions). Ce type de services permet à la personne publique de s'affranchir des contraintes liées à une infrastructure informatique complexe (il suffit de disposer d'un ordinateur, d'une tablette ou d'un smartphone connecté à internet) et aux services publics de gagner en efficacité.

Le recours au cloud pose néanmoins d'assez nombreuses questions auxquelles les personnes publiques doivent impérativement être attentives : la sécurité des données transmises et stockées dans le cloud est-elle assurée ? Le choix du modèle économique de certains prestataires est-il compatible avec le fait que les personnes publiques gèrent des données sensibles, personnelles et d'intérêt général ? Ces problématiques et d'autres sont à l'origine d'une nouvelle norme qui peut s'avérer fort utile aux acheteurs publics.

I. La normalisation du cloud computing

Le cadre réglementaire.

La directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données constitue aujourd'hui le texte de référence, au niveau européen, en matière de protection des données à caractère personnel. Elle met en place un cadre réglementaire visant à établir un équilibre entre un niveau élevé de protection de la vie privée des personnes et la libre circulation des données à caractère personnel au sein de l'Union européenne (UE) (1). En France, c'est la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés qui constitue le fondement de la protection des données personnelles. Elle a notamment été modifiée par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, qui a transposé la directive de 1995.

Il existe également plusieurs normes internationales en matière de sécurité de l'information, et notamment la norme certifiante ISO/CEI 27001 Management de la sécurité de l'information et la norme ISO/CEI 27002 Technologies de l'information/Techniques de sécurité/Code de bonne pratique pour le management de la sécurité de l'information.

Lire la suite….

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.courrierdesmaires.fr/46179/cloud-computing-et-marches-publics-garantir-la-confidentialite/

Reprenez le contrôle de votre identité en ligne avec IndieHosters

	**Reprenez le contrôle de votre identité en ligne avec IndieHosters**

Quand on s'inscrit avec un des géants du web comme Google ou Facebook, on souscrit à beaucoup plus qu'un seul service. On peut par exemple utiliser les mêmes identifiants pour s'enregistrer partout sur le web. C'est très pratique. Sauf que si votre compte se fait un jour pirater ou supprimer, vous perdez votre mail et tous les accès aux différents services que vous utilisez. IndieHosters veut vous aider à reprendre le contrôle de votre identité en ligne sans perdre le côté pratique.

Il existe de nombreuses alternatives aux identifications de Facebook et Google. Elles s'appellent OpenID ou Mozilla Personna. Le problème avec ces outils, c'est qu'ils demandent d'être hébergés sur un serveur en ligne et qu'ils doivent être régulièrement mis à jour. Les compétences techniques demandées dépassent bien souvent les bases des internautes avertis et c'est une galère qui décourage même les utilisateurs les plus motivés.
Aujourd'hui, si vous allez chez un hébergeur connu comme OVH ou Gandi, vous aurez droit en un seul clic à une adresse mail, un hébergement pour un site web, une base de données et WordPress ou quelques logiciels libres.
IndieHosters veut aller encore plus loin en proposant tous les outils qui vous permettent de gérer votre identité en ligne. Et pour garantir la confidentialité des données, ils vous offrent en prime un certificat TSL (identique à celui utilisé pour les opérations bancaires en ligne par exemple). Vos données vous appartiennent et elles ne sont pas accessibles pour l'hébergeur. Et comme vous bénéficiez d'un serveur chez IndieHosters, vous pouvez également en profiter pour créer votre blog.
Quand vous souscrivez chez IndieHosters, le serveur se trouve chez une personne et vous pouvez déménager de serveur en allant chez quelqu'un d'autre en un seul clic. Pour l'instant, ils ne sont que 2 chez IndieHosters : Pierre Ozoux et Michiel de Jong. Dans les mois qui viennent, IndieHosters accueillera de nouveaux hébergeurs indépendants et proposera de plus en plus de logiciels libres accessibles et administrables par des débutants, comme Owncloud, la solution alternative à Dropbox.
Pour se développer, ils ont lancé une campagne de financement participatif sur IndieGogo. Et j'ai rencontré Pierre Ozoux alors qu'il était de passage à Toulouse pour qu'il m'explique son projet.
Le but avoué d'IndieHosters est que chaque personne puisse créer son propre nom de domaine, son adresse email, son système d'enregistrement en ligne et finisse un jour par quitter Google, Facebook et consorts. Si vous voulez rejoindre ce mouvement, dépêchez-vous, la campagne de financement se termine dans quelques jours seulement.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.gizmodo.fr/2014/12/18/reprenez-le-controle-de-votre-identite-en-ligne-avec-indiehosters.html

---

Un label qualitatif pour le Cloud

Un label qualitatif pour le Cloud

Le 9 Décembre 2014, le label « Cloud Confidence » a officiellement été lancé par l'association du même nom. Cette certification est destinée à certifier la qualité d'un service Cloud en matière de sécurisation et de confidentialité des données et ne sera délivrée qu'à des offres à destination d'un des pays de l'Espace Economique Européen (EEE).

L'association « Cloud Confidence », fondée en Juillet 2014, est une association française qui regroupe 15 membres fournisseurs de services et de solutions cloud. Son but étant « de promouvoir la confiance dans les activités de Cloud entre professionnels et utilisateurs ».
Ce label « Cloud Confidence », centré sur la protection et la confidentialité des données clients, n'est pas la seule certification Cloud sur le marché français. Le réseau de clusters numérique « France IT » certifie depuis un an, les offres avec un point de vue généraliste. Plus proche du Cloud Confidence, le référentiel online publié par l'Agence Nationale de la Sécurité des Systèmes d'Information qui évalue le niveau sécuritaire des prestations Cloud.

Cette multiplication de labels prouve une nouvelle fois la place de plus en plus importante prise par le Cloud sur le marché des Télécoms depuis quelques années. Il est désormais presque indispensable pour une entreprise de sécuriser au maximum ses données et ce, en passant par une solution Cloud. Les nuages ne sont donc pas forcément annonciateurs de mauvais signes…

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.categorynet.com/communiques-de-presse/internet/un-label-qualitatif-pour-le-cloud-20141211224524/

Un « coffre-fort » en ligne pour le stockage des données

Un « coffre-fort » en ligne pour le stockage des données

L'Institut Hasso Plattner (HPI) de Potsdam (Brandebourg) et l'Imprimerie fédérale (Bundesdruckerei) ont convenu d'un partenariat de recherche. Dans le cadre d'un premier projet pilote, un « coffre-fort en ligne » sera développé et mis à la disposition du grand public, de l'administration et des entreprises. Ce système doit permettre à l'utilisateur de stocker et gérer ses données en toute sécurité.

Le HPI, centre de recherche sur les TIC créé et financé par le co-fondateur de l'entreprise SAP, apporte sa technologie « Cloud-RAID » [1]. Les techniques RAID, généralement appliquées aux disques durs, consistent à répartir les données sur plusieurs supports physiques distincts pour améliorer les performances, la sécurité ou la tolérance aux pannes du système. Cette architecture a été adaptée au cloud.

L'Imprimerie fédérale contribue au projet, quant à elle, avec sa plateforme « Trusted Service ». Celle-ci garantit l'identification fiable des utilisateurs du « coffre-fort en ligne » par un document d'identité. La solution, où les données ne doivent être visibles que par l'utilisateur concerné, doit être flexible et facile à utiliser. Plusieurs fournisseurs de cloud sont intégrés au projet, ce qui implique qu'aucun prestataire ne sera, seul, en possession de l'ensemble des données.

Le projet pilote court jusqu'en mars 2015. Afin d'intensifier les recherches en matière de la gestion de l'identité numérique, les deux partenaires prévoient la mise en place d'un laboratoire sur la sécurité au HPI.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.bulletins-electroniques.com/actualites/77364.htm

Juniper Networks présente ses prédictions réseau, cloud et sécurité pour l’année 2015

Juniper Networks présente ses prédictions réseau, cloud et sécurité pour l’année 2015

Bientôt, nous allons atteindre et même dépasser la barre des 5 milliards d'utilisateurs connectés. Il y a trente ans, l'innovation était un concept à sens unique, une démarche clairement orientée entreprises, où les consommateurs passaient au second plan. Depuis, les choses ont changé. Alors que près de la moitié de la population mondiale est connectée à Internet, les consommateurs ont désormais leur mot à dire et exigent des applications et services innovants pour la qualité de leur vie, à leur rythme et à leurs conditions.

L'environnent de l'entreprise est contraint d'évoluer au rythme des innovations, chaque année, plus nombreuses. Bruno Durand, vice-président TCC, EMEA, chez Juniper Networks a analysé les tendances 2015 dans les réseaux, le cloud et la sécurité. Il partage aujourd'hui ses conclusions avec vous.

Réseaux intelligents : La diffusion de contenu sème la confusion chez les câblo-opérateurs
Si la tendance est au numérique depuis plusieurs années, l'industrie du câble n'a pour ainsi dire pas évolué. Mais 2015 sera l'année du changement. Avec l'avènement et l'essor de la diffusion de contenu en streaming, les abonnés, qui se tournent vers différents fournisseurs de contenu comme Netflix, commencent à demander de nouveaux services à leurs câblo-opérateurs. Selon le rapport « U.S. Digital Video Benchmark » publié cette année par Adobe, le nombre des consommateurs de contenu en streaming a augmenté de près de 400 % depuis l'an dernier. Cette tendance devrait se poursuivre, et pour rester dans la course et gérer l'augmentation du trafic IP, les câblo-opérateurs devraient miser sur les réseaux virtualisés en 2015. Même si la transition durera plusieurs années, ils vont d'ores et déjà examiner les possibilités qui s'offrent à eux et commencer à lancer des appels d'offres pour trouver des fournisseurs partageant leur vision.

Le trading hypercontextuel (HCT) supplante le trading à haute fréquence
Passé de 7 milliards de dollars en 2008 à 1,4 milliard de dollars en 2013, le trading à haute fréquence est sur le déclin. Il représente à l'heure actuelle moins de 50 % des volumes d'activité des marchés financiers, contre 70 % en 2008. Le trading HCT (hypercontextuel) constitue le nouveau mouvement de dérèglement du marché. Il repose sur l'assimilation en temps réel des fils d'actualités classiques (Bloomberg, Thomson-Reuters, AP, CNN) et des flux des réseaux sociaux (Twitter, Facebook, LinkedIn, Blogs, etc.) en vue d'exploiter les informations du marché et d'acquérir un avantage concurrentiel en termes de transactions boursières. Le tout est piloté par des analyses permettant le chargement, le traitement et l'extraction rapides des données dans le but de tirer parti des discontinuités du marché. Le trading HCT relève de l'informatique distribuée et de la performance. La latence est le principal enjeu et ne constitue plus un facteur de différenciation. Un système extrêmement intelligent s'impose. Les entreprises et leur environnement informatique vont devoir pré-assimiler plusieurs centaines de flux d'informations en temps réel, ce qui nécessitera une programmation et un équipement réseau extrêmement pointus.

Big Data et réseaux : un bien ou un mal ?
Face à l'« Internet des objets », dont les tentacules (les terminaux) continuent de se déployer dans nos vies, les données générées vont être beaucoup plus nombreuses. Ainsi une simple connexion entre un téléphone et un système de sécurité résidentiel produira des données qu'il faudra bien stocker quelque part. En 2015, il s'agira à la fois d'analyser ces données, de les interpréter via une infrastructure réseau appropriée et de les sécuriser au moyen de technologies dédiées. Les entreprises et opérateurs de télécommunications revoyant leurs méthodes de développement de réseaux pour gérer la déferlante de données, la demande de spécialistes des données va atteindre des niveaux record.

Cloud : Des clouds privés d'un nouveau genre vont apparaître
Les entreprises hors de la sphère informatique habituelle exploiteront le cloud autrement pour proposer leurs produits et services. L'essor des paiements mobiles, la multiplication des équipements connectés et les questions de sécurité qui en découlent vont transformer les marchés verticaux de manière radicale. À l'instar de Nike, autrefois spécialisé dans les vêtements de sport et désormais marque lifestyle connectée avec ses dispositifs de suivi, ou de Starbucks, devenu un grand adepte des paiements mobiles et de la diffusion de contenu, nombre d'entreprises vont créer des clouds privés pour répondre aux exigences de leurs clients. Si le cloud, comme toute nouvelle technologie, était au départ l'apanage des chefs de file du secteur des hautes technologies (sites web, services financiers), les entreprises du monde entier et de tous horizons – par exemple, les compagnies pétrolières et gazières comme Hess – vont, elles aussi, pouvoir s'y mettre. En 2015, la création de clouds permettra de se démarquer dans tous les secteurs.

Les solutions SDN en 2015
Les réseaux SDN (Software-Defined Network) vont se multiplier, à mesure que le marché et la technologie gagnent en maturité et que de plus en plus d'entreprises prennent conscience de la valeur de ces solutions. Les entreprises françaises commencent à voir les avantages du SDN selon une étude publiée cette année par Juniper : automatisation accrue, sécurité renforcée et centralisation dans la gestion des ressources. Si, en théorie, ils peuvent faciliter la gestion des réseaux et réduire les coûts, qu'est-ce que les entreprises vont réellement en faire ? Le SDN (couplé aux analyses) procure l'agilité nécessaire pour fournir des services avant que les clients ne les réclament.

Sécurité : Le marché noir continue de gagner en maturité
Selon une étude réalisée par RAND Corporation et Juniper Networks, les marchés noirs de la cybercriminalité ont atteint un niveau de maturité significatif. Et, cette tendance devrait se poursuivre en 2015. Face à la vulnérabilité persistante des systèmes de point de vente et l'afflux de services cloud, les pirates motivés par l'argent ont de beaux jours devant eux.

De nouveaux outils de piratage et kits d'exploitation des vulnérabilités des systèmes informatiques devraient voir le jour. Par ailleurs, malgré les mesures de répression prises par les services de police à l'encontre des sites web frauduleux tels que Silk Road, de nouveaux marchés devraient se développer pour répondre à la forte demande d'enregistrements volés et autres biens illicites. Les principaux fournisseurs de cloud et sites marchands étant la cible d'attaques à grande échelle, le nombre de cartes bancaires et autres identifiants proposés à la vente sur le marché noir devrait demeurer significatif.

L'analyse des données s'étend à la sécurité
Face à la volonté permanente de fournir des renseignements mieux exploitables et de meilleure qualité sur les menaces, on peut s'attendre à une hausse de la demande de spécialistes des données dans le domaine de la sécurité (« Data Scientists »). Déjà fortement sollicités dans d'autres secteurs, les professionnels capables de fournir des données plus précises sur les menaces seront extrêmement recherchés. C'est en appliquant les meilleures pratiques de la science des données à la sécurité que les entreprises disposeront de renseignements fiables et utiles sur les pirates et leurs attaques, et parviendront à se démarquer.

Sécuriser l'Internet des objets
Face à la multiplication des équipements connectés à Internet, le nombre de pirates et d'attaques a de fortes chances d'augmenter. À l'ère de l'Internet des objets, les entreprises qui ne s'étaient jamais soucié de la sécurité de leurs logiciels ne vont plus pouvoir se voiler la face, sous peine de s'exposer à de lourdes conséquences. Les pirates capables de prendre le contrôle à distance d'équipements médicaux, de voitures, de thermostats et autres systèmes physiques représentent une menace de taille pour la société. Les sociétés qui développent ces technologies doivent désormais intégrer la sécurité dans leur processus et mettre au point des outils permettant de corriger rapidement les systèmes concernés. À défaut, les risques de piratage logiciel des environnements et systèmes physiques stratégiques seront bien plus nombreux.

Nette amélioration de la confidentialité des données des utilisateurs
La confidentialité des données jouera un rôle majeur dans le développement et l'adoption de nouveaux produits. Suite aux récentes révélations sur les programmes de surveillance à grande échelle des administrations et services de police, les individus sont nettement plus intransigeants sur la confidentialité de leurs données, et les sociétés l'ont bien compris. Apple a, par exemple, renforcé la sécurité de son nouvel iPhone et de son système d'exploitation en mettant au point un système de cryptage par défaut qui va jusqu'à lui interdire l'accès aux données en sa qualité d'éditeur. Résultat : il ne peut pas fournir d'informations sur ses clients à d'autres parties, comme l'administration, et les oblige ainsi à contacter directement l'utilisateur.

Outre la sécurité renforcée des produits grand public, les applications de communication respectueuses de la confidentialité vont commencer à se généraliser. Face à des utilisateurs soucieux de la protection de leurs données, les applications comme Wickr et Silent Circle vont gagner en popularité.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.globalsecuritymag.fr/Juniper-Networks-presente-ses,20141210,49338.html
par Juniper Networks

France Connect, pour simplifier l’administration numérique

France Connect, pour simplifier l’administration numérique

Les administrations et les collectivités locales qui bénéficieront à court terme d'un support d'identification unifié.

Thierry Mandon, le secrétaire d'Etat chargé de la réforme de l'Etat et de la simplification, s'est rendu le 2 octobre dans les locaux de la Dila pour visiter le plateau de développement du projet « France Connect ». France Connect est la « marque de fabrique » du futur système numérique national d'identification et d'authentification des usagers des services de l'administration.
Le dispositif, développé par le Secrétariat général pour la modernisation de l'action publique (SGMAP), cible les services publics de l'Etat, les administrations et les collectivités locales qui bénéficieront à court terme d'un support d'identification unifié, bon marché et relativement facile à implémenter dans leur propre système d'information.
Ce programme, qui sera déployé dès 2015 avec la bascule sur France Connect des trois millions de comptes du site portail « mon.service-public.fr », doit permettre à l'usager de fédérer tous ses comptes publics existants, puis d'établir ensuite de nouvelles connexions avec des administrations non encore dotées de leur propre système d'authentification, à condition d'adopter directement celui de France Connect.

La solution annule et remplace la carte d'identité électronique
La procédure qui s'apparente à celle déjà pratiquée par les réseaux sociaux comme « Facebook Connect » ou « Google+ Sign in » restera relativement simple à déployer. L'usager n'ayant pas encore de compte pourra s'enregistrer à partir d'une administration reconnue par le label et à laquelle il est numériquement affilié. Après avoir saisi ses identifiants d'origine, le site lui proposera en retour de fédérer son compte avec France Connect.
Après avoir donné son consentement, il disposera d'un compte national réutilisable sur de nombreux sites. Cette simplicité dans le mode d'enregistrement a d'ailleurs incité la DGFIP à proposer aux contribuables, dès la campagne 2016 de déclaration de revenus en ligne, de fédérer leur compte « impôts.gouv.fr » avec France Connect afin d'étendre rapidement le dispositif aux 10 millions d'utilisateurs dotés d'un compte fiscal.
France Connect ne se limite pas au seul composant unifié d'identification. A terme, il devrait permettre aux administrations et notamment aux collectivités d'effectuer des requêtes sur le niveau d'imposition ou sur la domiciliation de l'usager afin d'éviter l'étape coûteuse des demandes de justificatifs. Selon un expert ayant participé à la définition du projet, la nouvelle solution répondrait à 95% des besoins justifiant la création d'une carte d'identité électronique (CNIE) et l'économie réalisée sur la « non création » de cette carte avoisinerait le milliard d'euros.
France Connect devrait ainsi accélérer le développement de portails de téléservices couvrant la totalité des besoins transactionnels des collectivités avec les usagers et constituer également une brique essentielle de la mise en œuvre du programme « dites-le nous une fois » dans toutes les administrations. Autant dire qu'il constitue déjà à lui seul un levier essentiel pour les prochaine conquêtes de l'administration numérique.
Philippe Parmantier / EVS

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.localtis.info/cs/ContentServer?pagename=Localtis/LOCActu/ArticleActualite&cid=1250267813817

Le travail du futur va

s’appuyer sur le numérique et le partage de données

	Le travail du futur va s’appuyer sur le numérique et le partage de données

Le travail et son environnement évolueront dans les années à venir avec l'utilisation grandissante de la technologie. Le partage des données avec son employeur constituera un enjeu.

Les avancées technologiques auront un impact conséquent sur le monde du travail dans les cinq à dix années à venir, c'est l'avis que partagent 53% des personnes interrogées par PwC lors de sa dernière étude portant sur le devenir du travail en 2022. 10 000 employés ont été interrogés en Allemagne, Chine, Etats-Unis, Inde et Royaume-Uni, ainsi que 500 professionnels des ressources humaines, afin de recueillir leur point de vue sur l'évolution de leur lieu de travail et le management de la main-d'œuvre. Si les innovations technologiques auront le plus gros impact sur la manière de travailler dans le futur, la gestion des ressources climatiques, économiques et démographiques influenceront également – quoique dans une moindre mesure – le travail des employés interrogés.

Le partage des données comme outil de performance
Point sensible mais nerf central, l'utilisation des données personnelles par l'employeur dans le but d'améliorer la performance des employés et mieux comprendre leurs motivations au travail. Presqu'un tiers des sondés n'y sont pas opposés dès lors que les données personnelles se résument à leur profil sur les réseaux sociaux ou leur profil de santé. Une proportion liée à l'arrivée dans la décennie à venir de la génération Y sur le marché du travail, et qui constituera la moitié de la main-d'œuvre d'ici à 2022. Cette génération est particulièrement à l'aise avec le partage de ses données pour l'amélioration de son mode de travail. A terme, à l'instar des commerçants qui collectent des informations sur leurs clients pour offrir une meilleure offre, les entreprises collecteront des données sur leurs employés.

L'impact du numérique, positif ou négatif ?
Plus de la moitié des sondés (64%) considèrent que les technologies constituent un moyen d'améliorer les perspectives d'emploi. L'utilisation du numérique a un impact sur les horaires de travail classiques qui se trouvent bouleversées. Cela apporte flexibilité au travail mais le revers de la médaille se ressent sur la séparation vie professionnelle/vie privée. Ainsi, 59% des sondés disent être joignables à tout moment afin de s'assurer un poste ou une embauche. Concernant les employés de la génération Y, 64% partagent cet avis. La technologie n'est pas seulement source d'opportunités, et certains la considèrent comme une menace puisqu'un quart des sondés pense que l'automatisation des tâches pourrait avoir un risque sur leur poste.
Par Eliane HONG 01 septembre 2014

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.atelier.net/trends/articles/travail-futur-va-appuyer-numerique-partage-de-donnees_431005

73% des entreprises ne sont pas prêtes après un sinistre

dans le cloud

73% des entreprises ne sont pas prêtes après un sinistre dans le cloud

Avec des applications de plus en plus hébergées dans le cloud, les entreprises doivent faire évoluer leurs plans de reprise d'activité suite à un incident ou une panne. Mais pour Carlos Escapa, SVP chez Unitrends, la prise de conscience est encore incomplète.

L'utilisation massive du cloud pour héberger les applications critiques des entreprises multiplie les risques en cas de sinistre sur les équipements. Or, les entreprises ne semblent pas prêtes dans ce scénario à restaurer rapidement l'activité. Telle est la conclusion d'une étude mondiale menée pour Unitrends, un spécialiste des plans de reprise d'activité.
Les chiffres sont assez parlants : 78% des personnes interrogées ont connu des coupures des applications critiques, dont 63% estiment que les pertes ainsi engendrées vont de quelques centaines de dollars à plus de 5 millions. 28% des entreprises touchées par un incident estiment que leurs entreprises ont été privées de fonctions clés de leurs datacenters pendant des périodes pouvant aller jusqu'à plusieurs semaines.
« Le phénomène est particulièrement prégnant en Amérique du Nord où les ruptures d'alimentation énergétique des datacenters sont fréquentes. Mais on peut aussi évoquer la complexité de la cartographie applicative et les erreurs humaines », explique à ZDNet.fr, Carlos Escapa, SVP chez Unitrends.
Or, 73% des entreprises déclarent ne pas prêtes pour la restauration après sinistre. 64% des personnes interrogées estiment que le budget alloué par l'entreprise au plan de restauration après sinistre est inadapté et insuffisant. Et plus de 60% estiment qu'elles n'ont pas complètement documenté leur plan de reprise d'activité. Parmi la minorité qui dit l'avoir correctement renseigné, 23% n'ont jamais testé ces plans de reprise d'activité.

78% des entreprises interrogées ont subi des coupures dans les applications critiques
Evidemment, ces chiffres alarmants sont à relativiser étant donné que la source de cette étude n'est autre qu'un fournisseur de solutions dédiées aux PRA (plans de reprise d'activité) issus d'environnements virtualisés. Mais ils illustrent une tendance : le passage des applications critiques dans le cloud n'a pas été suivi d'un adaptation des PRA.
« Les pannes de service ne sont pas tolérables, encore moins aujourd'hui avec des processus qui s'appuient sur des applications, notamment mobiles », ajoute le responsable. « La protection des données ne suffit pas et les directions prennent conscience de l'importance de PRA adaptés ».
Cette prise de conscience est désormais en progressions dans les directions et les DSI « car les applications mobiles sont au coeur du business », résume prosaïquement Carlos Escapa. « Et puis, il y a la pression des contraintes légales comme Bâle 2 qui impose à certains secteurs des politiques précises en matière de panne ».
Pour autant, le chiffre de 73% d'entreprises pas prêtes paraît colossal. « Cela ne nous étonne pas. La plupart des PME estime que les PRA sont trop coûteux et estiment mal le risque financier de sinistre dans les datacenters. Notre discours est de dire qu'avec le cloud, le ticket d'entrée est moins élevé, ce qui permet d'adresser les entreprises plus petites ».
L'argumentaire est d'autant plus complexe à tenir qu »il n'y pas moyen de calculer le ROI d'un projet PRA », reconnaît notre interlocuteur. Tout en précisant « qu'en France, la prise de conscience est forte ».
Unitrends, qui affiche un chiffre d'affaires de 65 millions de dollars (+57% sur un an) indique protéger 1 exabyte de données dans le monde, et ses technologies de backup permettent de garantir un rétablissement après sinistre de une heure.
Par Olivier Chicheportiche | Lundi 01 Septembre 2014

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.zdnet.fr/actualites/reprise-d-activite-73-des-entreprises-ne-sont-pas-pretes-apres-un-sinistre-dans-le-cloud-39805553.htm

---

5 conseils pour protéger ses photos et données perso dans

le cloud

5 conseils pour protéger ses photos et données perso dans le cloud

Chiffrement, mot de passe et bon sens commun sont les meilleures armes pour protéger ses données dans le cloud. Même si le risque zéro n'existe pas.

Avec le piratage des photos nues de stars féminines, le problème de la sécurité des services cloud se rappelle à notre bon souvenir. Externaliser le stockage de ses données auprès d'un service en ligne peut être très pratique, mais cela présente aussi des risques, et même de plus en plus. Lors des dernières conférences de sécurité BlackHat et Defcon à Las Vegas, les experts en sécurité sont d'ailleurs unanimes à ce sujet : à force d'interconnecter de plus en plus de services en ligne et d'objets, on augmente la surface d'attaque, et donc le risque de se faire pirater. « Un bon hacker suffisamment motivé peut pirater presque n'importe quoi aujourd'hui », estime même Dan Geer, un expert américain reconnu en sécurité informatique.
Mais alors, le combat est-il perdu d'avance ? Par forcément, car il existe un certain nombre de règles de bons sens qui permettent quand même de limiter le risque.

1) Evitez le cloud pour stocker des données confidentielles. Stocker ses photos sur iCloud ou Google Drive, c'est très pratique, notamment pour les synchroniser et les partager avec vos amis. Mais, de grâce, n'y mettez pas les clichés de vos derniers ébats sexuels. Vous pourriez le regretter.

2) Utilisez un bon mot de passe. Certains experts pensent que le service d'Apple a été victime d'un attaque par force brute, c'est-à-dire le test une par une de toutes les combinaisons possibles (voir ci-dessous). Avec un mot de passe tel que « 0123456 », votre compte explose en quelques secondes. Choisissez, de préférence, une suite aléatoire de chiffres et de lettres. Evidemment, il est impossible de s'en souvenir, c'est pourquoi il faut utiliser un gestionnaire de mots de passe tel que 1pass ou LastPass.

3) Chiffrez vos données. Si vous avez des données confidentielles et que vous voulez quand même utiliser le cloud, il y a une solution : le chiffrement préalable. Les données sont d'abord cryptées par un logiciel tel que TrueCrypt, puis envoyées vers le service de stockage en ligne. Même en cas de vol, les données sont (théoriquement) inutilisables. Certains services en ligne, comme SpiderOak, intègrent d'emblée cette procédure de chiffrement, la rendant plus simple d'usage (technologie Zero-Knowledge). Le revers de la médaille est que le chiffrement n'autorise pas certaines fonctionnalités très pratiques comme le partage ou la modification en ligne. Il faut faire un choix…

4) Analysez la sécurité de votre fournisseur. Tous les fournisseurs cloud ne sont pas au même niveau technologique. Certes, tous utilisent au minimum le chiffrement HTTPS, mais qu'en est-il du chiffrement des communications entre les datacenters (comme l'ont implémenté Google et Yahoo désormais) ? Le fournisseur propose-t-il l'authentification à deux étapes (comme Twitter, Google + ou Apple) ? Utilise-t-il la technologie Perfect Forward Secrecy pour blinder encore plus ses communications chiffrées (comme Microsoft ou Twitter) ? Cette analyse n'est pas aisée à faire, mais elle s'impose dès lors que les données sont sensibles.

5) Ne partagez pas tout avec n'importe qui. Le niveau de sécurité de vos données est égal au plus bas niveau de sécurité mis en place par vos amis avec qui vous les partagez. C'est le principe du maillon faible. Donc, sélectionnez bien les amis avec qui vous partagez vos photos confidentielles. Evitez, par exemple, d'inclure votre ex-petit ami(e) dans la liste…
Gilbert Kallenborn01netle 02/09/14 à 15h09

Pour information, Denis JACOPINI et son équipe proposent des solutions pour protéger vos données :
– protection contre la perte de données
– protection contre la fuite de données
– cryptage de clés usb, d'ordinateurs, d'espace Cloud ou de données
– renforcement des autorisations (sécurité avancée par SMS, biométrie…)
Audit – Conseils – Sensibilisation/Formation des utilisateurs à la sécurité informatique
Contactez-nous

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.01net.com/editorial/625810/vol-de-photos-de-nus-5-conseils-pour-proteger-ses-donnees-dans-le-cloud/#?xtor=EPR-1-NL-01net-Actus-20140902

Et si le Cloud ne respectait

pas vos données personnelles ?

	**Et si le Cloud ne respectait pas vos données personnelles ?**

Seulement 1% des fournisseurs de Cloud est prêt pour la prochaine loi UE La grande majorité des fournisseurs de cloud ne sont pas encore préparés à répondre aux exigences de la nouvelle directive sur la protection des données, dite « EU General Data Protection Regulation », qui devrait entrer en application l'année prochaine. Une loi qui remplacera l'ancienne directive de 1995 sur la protection des données (EU Data Protection Directive).
Selon les conclusions d'une étude réalisée par le spécialiste de la sécurité de Skyhigh Networks, seulement 1 fournisseur de services cloud sur 100 est prêt pour respecter la nouvelle directive portant sur la protection des données. Une loi qui entend moderniser l'ancienne régulation pour s'aligner sur les contraintes imposées par Internet et le Cloud.
La nouvelle directive, qui devrait être votée en 2014 pour une implémentation en 2015, impose aux contrôleurs des données (les entreprises propriétaires des données), à ceux qui traitent les données (tels que les fournisseurs de cloud et les hébergeurs) de **partager leur responsabilité en matière de fuite de données et de violations de la loi**.
Cette nouvelle loi s'appliquera aux entreprises européennes qui traitent des données personnelles et aux entreprises hors de l'Europe, qui contrôlent les citoyens européens ou traitent des données personnelles obtenues à partir de biens ou de services offerts aux citoyens européens.
Un examen de plus de 7 000 services cloud, effectué par Skyhigh Networks , a ainsi révélé que les fournisseurs ont des problèmes évidents avec les contraintes imposées par la nouvelle loi, notamment au sujet de la résidence des données, de la détection et de la notification des fuites de données, du chiffrement et des politiques de suppression des données (le droit à l'oubli).
« Il est sidérant de constater que peu de fournisseurs cloud sont préparés aux nouvelles régulations européennes, mais heureusement, il reste encore du temps pour se mettre en conformité. Cela implique de résoudre dès maintenant un certain nombre de problèmes, comme le droit à l'oubli, et d'implémenter des politiques de protection des données qui soient conformes à ces nouveaux standards », affirme Charles Howe, directeur de Skyhigh Networks pour l'Europe.
Cette nouvelle loi vise également à renforcer la confiance des consommateurs et des entreprises dans l'économie numérique en Europe.
« Pour les fournisseurs de cloud, cela implique inévitablement des ressources ainsi que des dépenses supplémentaires, mais ce n'est rien comparé aux pénalités pour violation de la loi, qui peuvent atteindre jusqu'à 5% des revenus annuels d'une entreprises ou jusqu'à 100 millions d'euros. »
Ce qui tranche avec la directive de 1995 qui ne comportait aucune démarche en matière de pénalités. Ces lourdes amendes vont transformer la protection données en un enjeu crucial et obligeront les entreprises à passer en revue ce qu'elles doivent faire pour se mettre en conformité, soutiennent quelques experts.

Le droit à l'oubli – un parcours difficile
L'un des amendements les plus controversés est le droit à l'oubli – les individus ont le droit civique de demander que leurs informations personnelles soient supprimées d'Internet. « Il s'agit d'un problème complexe, mais étant donné l'intérêt des medias, il est peu probable que les fournisseurs de cloud soient pris par surprise », explique Howe.

« Un gros problème est que 63% des fournisseurs cloud conservent leurs données indéfiniment et n'ont aucune disposition en matière de rétention des données dans leurs conditions de vente », ajoute-t-il.

Une autre donnée vient s'ajouter : **23% des fournisseurs cloud gardent la notion de droit de partager les données avec d'autres entreprises tierces dans leur condition de vente**. Ce qui complique un peu plus le fait de garantir la suppression de toutes les données, a également révélé l'étude. « Il est juste de dire que le droit à l'oubli peut s'avérer être un vrai parcours du combattant pour de nombreuses entreprises – les fournisseurs de cloud eux-mêmes et leurs clients. Il ne s'agit pas que d'un problème pour Google », soutient Howe.

L'étude rapporte également que seulement 11 pays sont conformes aux contraintes de l'UE en matière de résidence des données. La loi impose que les entreprises ne stockent ni ne transfèrent des données dans des pays hors de la zone européenne qui n'ont pas de standards équivalents en matière de protection des données.

La question de la résidence des données se pose également pour fournisseurs de cloud avec des datacenters dans le monde, qui dans leurs opérations courantes peuvent transférer ou stocker des données dans des pays qui ne sont pas conformes aux règles européennes. Les Etats-Unis, où 67% des datacenters pour le cloud sont localisés, font partie de ces 11 pays.

La résidence des données sera une difficulté clé pour les services cloud lorsque la nouvelle loi entrera en vigueur – puisque seulement 8,9% des fournisseurs américains disposent de la Safe Harbour Certification, qui les exempte de cette contrainte, soutient Skyhigh Networks.

« Un brouillon de **la nouvelle loi obligeait les entreprises à notifier aux autorités européennes dans les 24 heures, une fuite de données**, même si celle-ci est intervenue dans un service cloud tiers. Le problème tient au fait que de nombreux fournisseurs de cloud tiennent expressément responsable le client de la détection de faille et cela peut être une opération impossible », ajoute encore Howe.

« Certaines régulations en place, comme au Royaume-Uni ou en France, permettent aux entreprises de contourner les contraintes liées à la notification de failles, si les données sont rendues inaccessibles via le chiffrement. Malheureusement, seulement 1,2% des fournisseurs de cloud propose la gestion des clés de chiffrement nécessaires pour cela », commente-t-il.

« La difficulté est que seuls quelques fournisseurs de cloud proposent des outils pour protéger nativement les données. En fait, seulement 2,9% des services cloud ont en place un système de mots de passe sécurisés. « La General Data Protection Regulation n'entre pas en application avant 2015, mais il reste encore beaucoup de travail à accomplir jusque-là », conclut Howe.

Lien pour télécharger l'étude :
http://info.skyhighnetworks.com/Cloud-Adopt–Risk-Report-July-2014_Registration.html

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :
http://www.lemagit.fr/actualites/2240226789/Protection-des-donnees-1-fournisseur-de-cloud-sur-100-pas-pret-pour-la-prochaine-loi-UE