

<http://www.lenuveleconomiste.fr/security-as-a-service-3555/>

Forum Gi

Gestion Institutionnelle Et Épargne Long Terme

Mutations, risques et opportunités

Le monde n'attend pas !

Le nouvel Economiste.fr

Publicité

Certificats Bonus et Bonus Cappés
Le CAC 40^e en plus tendance
Produits non garantis en capital



Nous contacter

Politique Economie Social Administratif Judiciaire Intellectuel Spirituel Médiaétique
Dév. Durable Droit Finance Management Marketing Services généraux Stratégie Technologie

Les archives

consultation gratuite



- LE JOURNAL
- LES ANALYSES
- LES DOSSIERS
- LES PORTRAITS
- LE "MANAGER DE L'ANNEE"
- LES CAHIERS THEMATIQUES
- CHRONIQUES
 - Alain Bauer
 - Henri Nijdam
 - Henry Laurent
 - Jean-Pierre Patat
 - Michèle Cotta
 - Pascal Lorot
 - Paul-Henri Moinet
 - Philippe Barret
 - Philippe Delmas
 - Pierre Kosciusko-Morizet
 - Sylvie Pierre-Brossolette
 - Xavier Raufer
- ENTREPRISES
 - Assurances
 - Commercial
 - Communication
 - Consulting
 - Création d'entreprise
 - Développement durable
 - Digital
 - Droit
 - e-commerce
 - e-marketing
 - Environnement
 - Export
 - Finance
 - Franchise
 - Gestion
 - Immobilier
 - Informatique
 - Logistique
 - Management
 - Marketing
 - Prévoyance
 - R&D
 - Ressources humaines
 - Services généraux
 - Stratégie
 - Technologies
 - Transports
 - Veille
- ART DE VIVRE & ENTREPRISE
 - Art

Information & technologies - Security-as-a-Service

La sécurisation informatique s'externalise aussi

> Lire en format journal

Cloud computing, Saas, normes PCI-DSS, piratage, externalisation. Une infrastructure informatique en cloud offre, intrinsèquement, un meilleur niveau de protection. Mais elle n'est pas pour autant totalement sécurisée. Comme tout service externalisé, le cloud doit être cadré par un contrat bien réfléchi. De plus, comme tout système informatique, il doit se protéger contre les attaques malveillantes et les négligences, qu'elles soient externes ou internes. La solution est de recourir à des tiers auditeurs, un rôle rempli par les spécialistes de la sécurité informatique, qui se lancent de plus en plus dans la prestation de service.



Assurer la sécurité informatique d'une entreprise est une affaire de plus en plus complexe. Une infrastructure informatique et les fonctionnalités qui y sont hébergées sont une combinaison d'éléments multiples, qu'il faut sélectionner, installer, et intégrer. "Maintenant, il faut sécuriser tout cet ensemble d'éléments totalement hétérogènes, qui bougent tout le temps, mais à leur propre vitesse", explique Philippe Courtot, CEO de Qualys. Le cloud se présente comme une alternative intéressante car elle apporte une simplification bienvenue.

"Quand on parle de datacenters de grande taille, la capacité de résilience [capacité de l'ensemble du système à supporter les opérations de maintenance et à gérer les incidents, en assurant un fonctionnement perçu comme normal et satisfaisant, NDLR] est largement au-dessus de la moyenne, indique Bernard Ourghanlian, directeur technique et sécurité chez Microsoft. De plus, la localisation des datacenters répond à ces contraintes spécifiques en termes de risques sismiques ou encore électriques : un système de batteries et de générateurs diesels assure une alimentation en énergie continue." Le coût de tels systèmes, ainsi que le coût de la main-d'œuvre en charge de la sécurité de l'infrastructure sont encore très élevés, trop élevés pour le budget des TPE notamment. Et ce quel que soit le domaine, sécurité physique ou sécurité virtuelle des données.

"On a tendance à considérer que la sécurité est toujours un obstacle au cloud computing, remarque Bernard Ourghanlian. Il y a des raisons contre, mais dans le même temps, le cloud assure un niveau de sécurisation supérieur à celui que l'on peut avoir en local." Ce qui ne veut pas dire que le cloud est la panacée en terme de sécurité, ou encore que tous les cloud sont égaux. "Il faut adapter la sécurité au système, et cela reste vrai pour le cloud, souligne Thibault Chevillotte, senior manager chez Logica Business Consulting. Ce dernier n'est pas monolithique, chaque modèle a une certaine capacité en terme de risque, de niveau de contrôle..." Il faut faire un choix. Par exemple, en Saas (Security as a Service), l'entreprise n'a quasiment plus rien à faire car les décisions sont dans les mains du prestataire. C'est une question de confiance, et ce quel que soit le fournisseur. "Il y a un choix fondamental à faire au départ, insiste Thibault Chevillotte. Et pour le guider, il faut faire une analyse de risque, et il n'est pas inutile d'être accompagné."

Contractualiser la localisation des données

Un des premiers éléments qui permet d'établir cette confiance est de savoir exactement quelles sont les prestations garanties par le contrat. En effet, comme il n'existe encore que peu de cadres légaux, la répartition des rôles et responsabilités incombe entièrement au contrat conclu entre le client et son fournisseur. "S'il arrive de perdre des données sensibles, c'est l'entreprise qui est responsable, rappelle Samir Koleilat. Elle est tenue de se renseigner sur les garanties contractuelles proposées par le prestataire." Ainsi, certains fournisseurs de cloud ne localisent

Rechercher

Lire en format journal



Cahier 1 Cahier 2

S'abonner



Les plus lus depuis une semaine

Communication - Le Brand Content

A la Une également - Capitalisme souverain

Sous la ceinture

A la Une - Le bazar de l'hôtel de vie

Qui recrute dix fois plus ?

A relire à propos...

De l'Islam en France

De la convergence franco-allemande et du pacte de compétitivité

Le nouvel Economiste

Le journal en résumé

La rédaction

La publicité

Les annonces légales

Les partenaires

Bernard Zimmern bourse Cloud computing
Delphine Manceau e-learning ERP ESCP
Europe Expatriation François d'Aubert
François de Witt free cash-flows Grenelle
Il Guy Pignolet Hard close Islam Jean-Marc
Ayrault Jean-Marc Sauvè Jean-Paul
Fitoussi Jean-Pierre Joui Jean-Robert
Pitte Jean Tulard Mandat ad hoc Marine
Le Pen Mediator Merkel MSN Europe

Nicolas Sarkozy

Olivier Pastré Outsourcing page rank
plateformes collaboratives Search engine
optimization Services VIP social search
Team building
WP Cumulus Flash tag cloud by Roy Tanck and
Luke Morton requires Flash Player 9 or better.

<http://www.lenouveleconomiste.fr/security-as-a-service-3555/>

- Automobile
- Gestion de fortune
- Luxe
- Patrimoine
- Spectacle
- Tourisme
- Vins & spiritueux
- AFFAIRES PUBLIQUES
-
- Economie
- Politique
- Social
- Sociétal
-
- Collectivités
- Etat
- Gouvernement
- Institutions
- Parlement
- Partis
- Présidentielles
-
- Administration
- Affaires étrangères
- Afrique
- Agriculture
- Allemagne
- Aménag. du territoire
- Asie
- Budget
- Capitalisme
- Chine
- Communication
- Culture
- Défense
- Démographie
- Emploi
- Energie
- Enseignement
- Etats-Unis
- Europe
- Fiscalité
- Formation
- Géopolitique
- Gouvernance
- Grande-Bretagne
- Grandes Ecoles
- Histoire
- Inde
- Industrie
- Intellectuel
- International
- Justice
- Libéralisme
- Marchés financiers
- Matières premières
- Médias
- Mondialisation
- Monnaie
- Moyen-Orient
- Outre-mer
- Pôles compétitivité
- Recherche
- Régions
- Religion
- Retraites
- Santé
- Sciences
- Sécurité
- Socialisme
- Spirituel
- Sports
- Universités
- ECONOMIE SOCIALE
-

pas leurs données. Or "il faut bien s'assurer de la localisation des datacenters où l'on est hébergé, insiste Samir Koleilat, PDG d'Acropolis Télécom. Par exemple, il faut que les deux cloud, indispensables pour assurer la redondance, soient éloignés de plus de 300 km, pour respecter les normes de protection contre les risques naturels." Mais ce n'est pas la seule raison qui pousse à s'interroger sur la localisation exacte de ses données. Il y a aujourd'hui un vrai questionnement sur le plan juridique. "Imaginons un prestataire de cloud américain, un client français, un datacenter en Irlande et un utilisateur en Chine, explique Bernard Ourghanlian. Chaque acteur se doit de respecter sa législation locale, mais pas les autres." Connaître la localisation de ses datacenters est une chose, protéger cette information confidentielle et stratégique en est une autre, tout aussi essentielle. L'hébergeur n'a pas le droit de divulguer le nom de son client, mais l'entreprise doit également cultiver la discrétion de son côté. "L'un des risques souvent mentionné, à savoir le fait que l'on ne sait pas où sont ses données, est de moins en moins vrai, tempère Loïc Guézo, directeur technique security solutions GTS IBM France. Cette réserve est surtout due aux premiers acteurs, tels que Google ou Amazon, dont l'architecture au départ n'était pas conçue pour la traçabilité des données. Mais ils y travaillent."

Autre exemple : la prise en compte des protocoles de sécurité que l'entreprise doit respecter, comme les normes PCI-DSS pour les transactions financières. Le fournisseur de cloud doit pouvoir assurer au minimum le même niveau de sécurité. "Enfin se pose le problème de la réversibilité, ajoute Thibault Chevillotte. Il faut s'assurer que les données peuvent être récupérées, notamment en testant cette fonctionnalité. Il faut aussi être capable de fournir des archives, si besoin." La récupération des données doit obéir à des critères précis, notamment en matière de format et de d'effacement final chez le prestataire. Tout cela suppose un certain niveau de coopération dans la durée, ou au moins d'entente, entre les différents acteurs du cloud.

L'herméticité des infrastructures en question

Outre ces risques liés aux prestations, l'infrastructure en nuage, comme toute infrastructure informatique, présente en elle-même des dangers potentiels. Si la plupart des risques "classiques", tels que la protection physique des datacenters, sont mieux contenus par les prestataires de cloud que leurs clients, le principe même d'une externalisation de la puissance informatique pose de nouveaux problèmes. "Le cloud vend des ressources, disponible à l'instant, précise Thibault Chevillotte. Et ces ressources sont partagées entre plusieurs clients. Du coup se pose un risque de décloisonnement des environnements." C'est-à-dire qu'il existe un risque réel qu'un utilisateur passe par erreur sur le serveur virtuel d'un autre client... Mais il existe des solutions, des programmes de gestion notamment qui se chargent de garder chacun chez soi. Même si ces derniers sont éprouvés, ils ne sont pas pour autant à l'abri d'une défaillance. "Si on est sûr des systèmes VMWare, l'hermétisation des serveurs virtuels est presque totale, explique Samir Koleilat. Et techniquement, nous pouvons le prouver."

Par ailleurs, si l'informatique est externalisée, il faut bien que l'entreprise puisse communiquer avec elle depuis ses terminaux. Ce qui se fait par des interfaces de programmation, ou API (Applications Programming Interfaces). Or "il existe des problèmes de sécurité liés aux API qui gèrent la connexion entre le prestataire et l'entreprise, définit Thibault Chevillotte. Ils doivent être sécurisés, et ce des deux côtés." En effet, ces applications sont de plus en plus complexes, un résultat direct de la multiplication des points de contact entre l'entreprise et son informatique à distance. Et plus un programme est complexe, plus il présente de risques. Sans compter que l'entreprise peut se voir demander, par des prestataires tiers engagés pour d'autres services, de fournir les droits de ces APIs.

Une cible de choix pour les hackers

La multiplication de ces points de contacts entre le cloud et l'Internet est une véritable source d'inquiétude. "Les nouvelles vulnérabilités viennent de la présence obligatoire sur Internet, explique Philippe Courtot. Les applications Web sont écrites un peu par tout le monde, et il y est possible que quelqu'un s'infiltrer pour accéder à votre base de données. Les applications Web sont très poreuses. C'est là où opèrent les hackers les plus brillants et donc se déroulent les attaques les plus virulentes. Et les moyens de lutte ne sont pas encore très coûteux."

La capacité de calcul du cloud est d'ailleurs parfois utilisée par les hackers pour mettre en place des services - illégaux - qui permettent par exemple de casser des mots de passe. Et la capacité du cloud à délivrer de la puissance à la demande peut être intéressante pour eux. En outre, "le cloud apporte une certaine homogénéité dans les infrastructures", estime David Grout, ingénieur avant-vente chez McAfee. Autrement dit, le travail des hackers s'en trouve facilité. Il existe cependant une contrepartie : les opérations de maintenance, de récupération ainsi que les mises à jour peuvent être faites par tout le monde instantanément. Si le système est bien géré, les réactions sont rapides. Y compris pour des clients qui n'ont pas subi l'attaque, mais qui bénéficient, en quelque sorte, du malheur des autres.

Flux et réseaux



nous retrouver sur Facebook



nous retrouver sur Twitter



s'abonner à notre flux Rss

Publicitéécue

<http://www.lenouveleconomiste.fr/security-as-a-service-3555/>

Diversité

Ethique

Mécénat

Philanthropie

Prospective

RSE

Solidarité

-

Associations

Comité d'entreprise

Coopératives

Fondations

Mutuelles

ONG

Syndicats

"Le cloud peut paraître une cible naturelle d'attaques de hackers, pour la raison qu'il y a plus d'œufs dans le même panier, estime Bernard Ourghanlian. Mais c'est oublier qu'ils sont également beaucoup mieux protégés. Attaquer un cloud entier, c'est beaucoup de travail pour le hacker. Surtout qu'il existe d'autres moyens." Et le plus couramment utilisé est l'usurpation d'identité. Tout le système d'externalisation de l'informatique repose en effet sur la notion d'identité électronique. "Les firewalls nouvelle génération peuvent associer un utilisateur avec une application, permettant ainsi d'assurer une meilleure protection, précise David Grout. C'est une des clés de voûte du système." Il existe ainsi des applications à l'intérieur des datacenters, des équipements spécifiques et un niveau global de sécurité assuré par les pratiques de l'entreprise, mais "l'unique rempart reste le nom d'utilisateur et le mot de passe, insiste Thibault Chevillotte. Il faut donc qu'ils soient bien gérés. Des salariés viennent, d'autres partent, cela peut poser un problème. La gestion des identités doit être bien coordonnée entre l'entreprise et le prestataire de cloud computing."

Audit et certification, gage de fiabilité

Autre maillon faible de la chaîne : l'humain. "L'humain reste un facteur essentiel de la problématique de la sécurité", rappelle David Grout. La formation en interne reste primordiale, mais les technologies permettent aussi de multiples contrôles pour limiter le risque de l'erreur unique. Le choix du prestataire est donc capital, "il faut savoir avec qui l'on travaille, souligne Samir Koleilat. Les techniciens ont-ils la compétence et la fiabilité voulue ? Comment sont-ils contrôlés par l'opérateur, et sont-ils sous des conditions de confidentialité ? C'est important, car ils ont accès à l'administration des serveurs." Ce ne sont pas des questions nouvelles : elles se posent dès que l'on fait appel à un tiers. "Traditionnellement, dans le cadre d'un service externalisé, on va mettre des clauses d'audit dans le contrat, estime Thibault Chevillotte. Mais là se pose un problème d'échelle. Microsoft ne peut pas vraiment se permettre de se faire auditer par plusieurs dizaines de milliers de clients. La clause d'audit est plus réaliste chez un petit fournisseur." En effet, un cadre de référence émerge progressivement. De plus en plus d'instances publiques s'intéressent au sujet. Par exemple, l'ANSSI – Agence nationale de la sécurité des systèmes d'information – a publié un livre blanc sur les problématiques de sécurité et externalisation, avec un chapitre consacré au cloud. Des certifications – l'ISO 27 001 et les SAS 70 – valident le respect chez un prestataire de certaines règles et pratiques en matière de sécurité. "Des organismes qui réfléchissent à la sécurisation du cloud au sens large, par exemple le NIST, son équivalent européen l'ENISA, ou encore les éditeurs eux-mêmes, avec la CSA", souligne David Grout. Du coup, cela permet au fournisseur lui-même de se faire auditer régulièrement par un tiers reconnu, et d'afficher les résultats. Une démarche applicable par tous les fournisseurs, quelle que soit leur taille. "Cette capacité à faire intervenir des tiers auditeurs est essentielle", insiste Bernard Ourghanlian.

L'arrivée du Saas (security as a service)

Face à ces évolutions du paysage informatique, les acteurs spécialisés de la sécurité informatique s'adaptent et proposent de plus en plus de services à distance, construits eux-mêmes sur le modèle du software-as-a-service. "Nous sommes un service du cloud qui permet aux fournisseurs de cloud ou aux entreprises de s'assurer de leur sécurité, explique Philippe Courtot. L'idée est de proposer un audit de façon automatisée, depuis Internet. Et nous sommes indépendants." La formule offre plusieurs avantages aux entreprises. Le premier : le coût. "L'arrivée du Saas [security as a service], est due premièrement à la crise économique, explique David Grout. Déléguer sa sécurité permet de se reconcentrer sur son cœur de métier. C'est aujourd'hui une demande en croissance, qui n'existait pas vraiment jusqu'au milieu de l'année 2010." L'idée existait déjà avant. Mais les outils et services proposés sont de plus en plus complets. Des services de fédération d'identité ont émergé, qui permettent de se connecter une fois avec son identifiant, typiquement sur la page Web de l'entreprise, puis d'aller ensuite sur diverses applications partenaires sans reconnexion.

L'avantage de ces prestataires spécialisés, c'est qu'ils disposent des ressources qui leur permettent de rester efficaces. "La sécurité est une œuvre permanente, souligne Loïc Guézo. Le plus important est donc d'établir une collaboration entre différents partenaires, de tous types, et de s'appuyer sur des experts qui peuvent offrir aux entreprises le même niveau de compétence que les pirates." La collaboration augmente, y compris entre entreprises. "Au vu de l'ampleur prise par le problème, une seule société, quelle que soit sa taille, ne peut pas lutter seule", estime Philippe Courtot. Car trouver les personnes à même de faire ces analyses est très difficile, et les garder relève de l'exploit. Une solution repose sur la mutualisation des connaissances ; c'est ainsi que Qualys est en train de bâtir un "malware research portal", dont l'objectif est d'offrir à des chercheurs du monde entier de faire des analyses sur ces données.

Par Jean-Marie Benoist

