TELEHOUSE

HOME TO YOUR GLOBAL ICT SOLUTIONS

Livre Blanc Sécurité IaaS

INTRODUCTION

Les grandes tendances du cloud en 2017 [1]

La transition vers le cloud a pris de l'ampleur en 2016 et cette maturité s'accompagne aujourd'hui d'une prise de conscience par les entreprises. La DSI se transforme et les équipes s'y préparent. Elles adaptent leurs compétences par des formations axées sur la sécurité du cloud, les bases de données hébergées et les infrastructures en tant que **services**. Elles adoptent des pratiques agiles pour accélérer les projets telles que l'utilisation de serveurs hébergés à la demande. Les entreprises adoptent plus largement les approches hybrides avec des solutions à la fois sur site et dans le cloud.

L'utilisation d'applications SaaS par les utilisateurs métier constitue un challenge pour la DSI. Celle-ci prend désormais l'initiative avec une approche proactive dans la sélection et la prise en charge de ces applications. La DSI garde ainsi le contrôle sur les applications installées et hébergées sans limiter les choix personnels des utilisateurs finaux. Une gouvernance bénéfique pour tous.

Les applications hébergées rationnalisent les opérations en réduisant les coûts et permettent de gagner en agilité. La DSI peut désormais se focaliser sur l'innovation et la production d'informations exploitables. Le cloud rapproche également les prestataires et les clients en réduisant les obstacles liés aux déploiements sur site et en favorisant la collaboration.

Les prestataires cloud permettent aux clients de s'affranchir de la complexité des législations locales. Leur rôle évolue et se focalise sur la conduite au changement.

Le marché de l'IaaS en plein essor

Selon les analystes, le marché de l'IaaS croît plus vite que celui du SaaS et est en plein essor en 2017 : +36,8% pour Gartner [2], +30,1% pour IDC [3] et +35% pour Forrester [4].

Une récente étude de Spiceworks montre que la plupart des entreprises utilisent déjà au moins un service cloud. Pour 1/3 des sondés, plus de la moitié des services IT vont migrer dans le cloud dans les 2 à 3 ans. Les services IT restent prudents lors de l'acquisition d'un service cloud émergent, mais sont toujours à la recherche d'un prestataire cloud dans le domaine de l'IaaS. [7]

Pour 93% des organisations, la sécurité reste toujours une des principales préoccupations selon Check Point. De ce fait, 47 % des professionnels en France ont ralenti leur adoption du cloud par manque de compétences pour en administrer la sécurité. Pour autant la confiance progresse : 62% des entreprises françaises stockeraient dans le cloud des données sensibles de leurs clients [5]. Car la sécurité du cloud progresse. Jusqu'en 2020, 95 % des défaillances de sécurité cloud seront du fait des clients et non du fournisseur, comme le prévoit Gartner [2]. Une nouvelle génération d'outils de surveillance renforce cette confiance dans le IaaS [6]. Le volume des attaques en ligne dépassera la capacité humaine à les traiter ; une automatisation des processus de sécurité deviendra indispensable. [6]

En 2017, la sécurité confirmera son rôle stratégique en aidant les RSSI à réduire les délais de commercialisation des produits et à assurer la confidentialité des données des clients et des employés. [8]

[1] https://www.tableau.com/sites/default/files/whitepapers/whitepaper_top_10_cloud_trends_2017_fr-fr.pdf
[2] http://www.gartner.com/newsroom/id/3143718
[3] http://www.idc.com/getdoc.jsp?containerId=prUS42321417
[4] http://www.networkworld.com/article/3151002/iaas/10-must-watch-iaas-cloud-trends-for-2017.html
[5] http://www.lemagit.fr/actualites/450415360/La-securite-reste-la-premiere-preoccupation-pour-le-passage-au-Cloud
[6] http://www.cloudmagazine.fr/avis-expert/les-10-tendances-cloud-securite-de-2017
[7] https://www.spiceworks.com/marketing/reports/it-cloud-services/
[8] http://www.zdnet.fr/actualites/tribune-securite-du-cloud-quelles-tendances-en-2017-39846470.htm

Les menaces de sécurité
et comment s'en protéger

Selon la Cloud Security Alliance, les menaces de sécurité sont les fuites de données, le vol de compte, le hacking d'interface et d'API, les cyberattaques, les pertes de données, le manque de sensibilisation et les abus des services cloud. On peut y rajouter également les employés malveillants.

Pour s'en protéger, il existe un certain nombre de méthodologies : *

- Les mesures de bases : au minimum, il faudra effectuer les mises à jour de logiciels planifiées, les procédures de patch, le monitoring et l'audit, des tests et des analyses de vulnérabilité réguliers.
- Les mesures de sécurité qu'offrent certains fournisseurs IaaS.
- Le chiffrement des données, une des méthodes les plus courantes pour protéger la confidentialité des données. Une protection que devrait vous fournir votre prestataire cloud pour accéder à vos machines virtuelles et à vos données clients.
- Le chiffrement du réseau qui est aujourd'hui un standard des infrastructures cloud.
- Le contrôle d'accès, que ce soit à travers le concept de cloud fédéré, d'un système d'authentification multi-facteurs (OTP, tokens, smartcards…), de pare-feu matériel ou logiciel…
- Le Cloud Access Security Broker (CASB), un outil de sécurité unifié
- Le contrôle de vulnérabilité, en conjonction avec des mises à jours logicielles régulières, est un must pour les fournisseurs et clients IaaS
- La surveillance active, l'audit et l'identification des anomalies en utilisant des techniques de Deep Packet Inspection (DPI), des solutions de détection d'intrusion (IDS) ou de prévention d'intrusion (IPS).
- La sensibilisation du personnel à travers des formations spécialisées et l'adoption d'une culture de la sécurité.

* http://www.esecurityplanet.com/network-security/iaas-security-threats-and-protection-methodologies.html

Une approche des risques
basée sur le modèle de partage des responsabilités

Le fournisseur cloud est responsable de la sécurité *du* cloud : infrastructure globale, stockage, bases de données, réseaux, calculs, pare-feu, … Le client quant à lui est responsable de la sécurité *dans* le cloud : données utilisateurs, plates-formes, applications, OS …, mais le fournisseur peut l'accompagner dans sa démarche de sécurisation.

Le plan d'actions à mettre en place est le suivant :

- Activation de l'authentification multi-facteurs
- Détection des accès complets sans restrictions
- Suppression des comptes inactifs
- Surveillance de la sécurité (comportements inhabituels, suractivité, tentatives de connexions par force brute…)

Que ce soit pour le IaaS, PaaS ou SaaS, les DSI doivent adopter des bonnes pratiques communes :

- Appliquer rigoureusement une composante IAM (Identity and Access Management)
- Chiffrer les données au repos
- Établir un nouveau plan de contrôle de sécurité pour accompagner les équipes dans la transition vers le cloud
- **Sauvegarder toutes les données**

Plus spécifiquement pour le IaaS, le client pourra également appliquer les bonnes pratiques suivantes :

- Assumer la responsabilité des instances et des applications
- Faire réaliser des audits de conformité (SOC 1/2/3, ISO 27001, PCI, FedRAMP, etc.) par des tiers

Les points de sécurité à vérifier
pour choisir un fournisseur IaaS

Système physique

- **Le site physique doit être protégé contre les intrusions** (intervenants non habilités, ...) et être auditable
- Hybridation : il doit proposer la possibilité de raccorder son cloud privé
- Sécurité/performance : **un accès au IaaS par réseau privé (MPLS, ...) doit être possible**

Système logique

- **L'authentification administrateur** doit se **faire à travers un VPN avec une double authentification**
- En cas de défaillance matérielle, la disponibilité et les performances doivent être assurées (fonctionnalités de **l'hyperviseur VMWare** par exemple)
- **Des protections** contre les attaques DDoS au niveau du backbone opérateur.
- **Le pare-feu managé** [avec Telehouse, 30% des paquets sont droppés par le pare-feu]
- La **charge répartie** sur plusieurs serveurs frontaux
- La **RAM toujours disponible en cas de surcharge** (pas de surbooking de RAM)
- Une **sauvegarde complète** quotidienne des VM à effectuer **sur une infrastructure dédiée**
- **L'étanchéité des données** entre clients hébergés doit être assurée
- **L'effacement des données certifié** en fin de contrat par outil spécialisé, avec mise à disposition de rapports d'exécution

Support technique

- **Le support intégré et effectué par le fournisseur cloud**, non par des sous-traitants

Réglementation

- La souveraineté **des données assurée : serveurs localisés** en France**, contrat rédigé en droit français et en fonction de la criticité de vos données non soumis à la législation américaine**
- Le fournisseur doit **posséder les certifications ISO 27001, 9001, PCI-DSS**, …

Services optionnels. Le fournisseur peut proposer en option

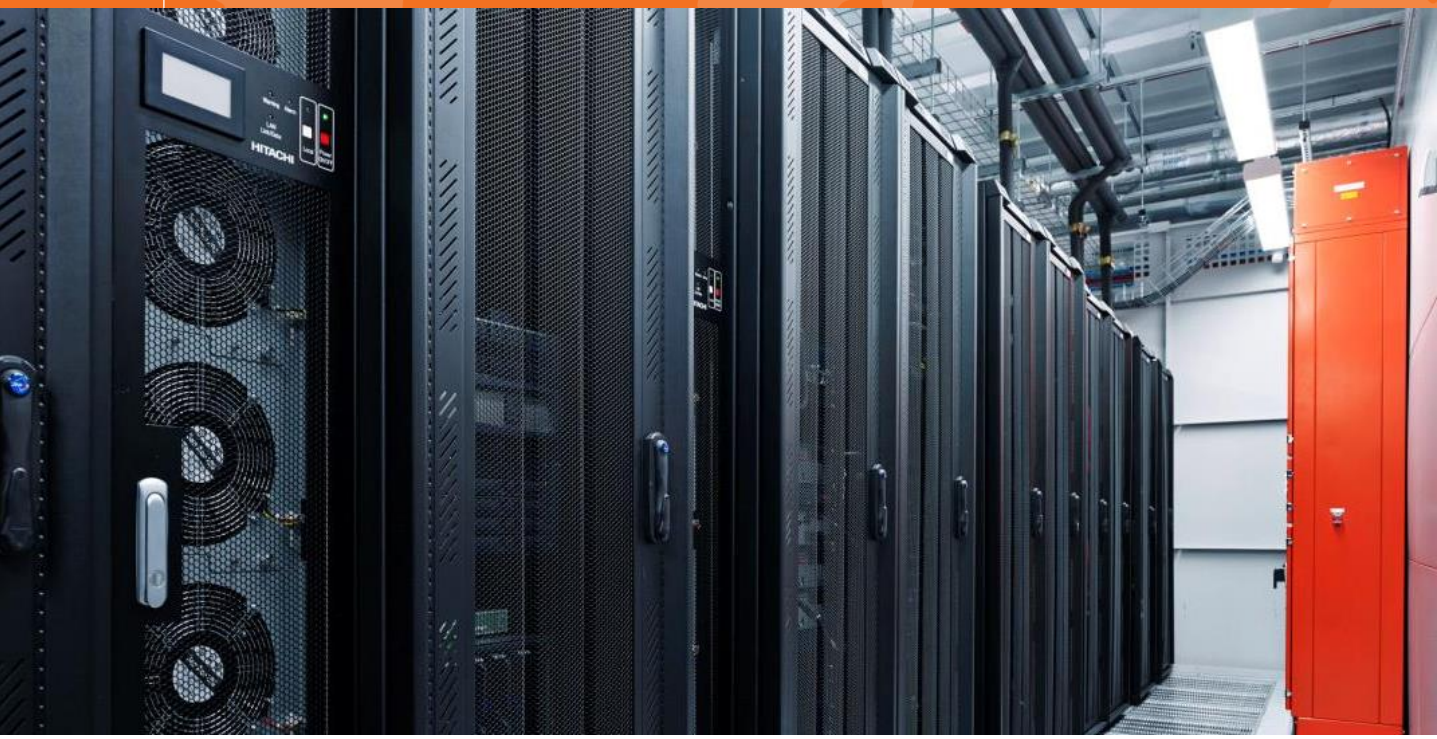
- Un antivirus
- La détection de vulnérabilité : diagnostic des failles
- Les tests de montée en charge
- Une supervision applicative : une surveillance de la disponibilité et la qualité des applicatifs
- Des tests de non-régression
- Une sauvegarde quotidienne granulaire (fichiers, emails, base de données) [50% des VM Telehouse ont cette option]
- Un Plan de Reprise d'Activité sur **site distant avec accès réseau indépendant** [30% des VM Telehouse sont fournies avec un PRA]

Il restera de la responsabilité du client :

- L'ouverture des flux internet vers les VM
- La sécurité logique : ouverture des ports du pare-feu
- Une politique de mots de passe complexes
- Le développement d'applications sécurisées
- L'architecture haute disponibilité : faire des demandes de VM en cluster réparties sur des serveurs physiques distincts
- L'infogérance applicative

CONCLUSION

L'adoption croissante des solution IaaS et la maturité croissante des entreprises ne doivent pas occulter le défi majeur du cloud : la sécurité. Le choix d'un partenaire de confiance (plus qu'un fournisseur donc) est primordial pour accompagner sa transformation numérique, notamment dans la complexité des services de sécurité et la mise en place des fonctions optionnelles parfois indispensables. Des équipes et des serveurs localisés en France sont les garants à la fois d'une conformité réglementaire et d'une qualité de support.



TELEHOUSE

HOME TO YOUR GLOBAL ICT SOLUTIONS

www.telehouse.fr