Le cloud d'entreprise pour assurer une transition numérique : 6 points de vigilance

OVHcloud

vmware®

Le cloud est désormais bien ancré dans les services informatiques de toutes les entreprises. Avec le développement de la transformation numérique dans tous les secteurs, les entreprises se tournent vers des stratégies multicloud pour s'adapter aux besoins du marché. L'un des éléments clés de cette approche est le cloud privé, considéré comme plus sécurisé que le cloud public[1].

Même si un cloud privé d'entreprise offre davantage de contrôle sur l'environnement physique et des possibilités de personnalisation uniques, construire votre propre cloud privé n'est pas sans risques...

Les failles de sécurité

Atteintes à la protection des données, vols d'identifiants, pannes d'authentification, piratages d'interfaces et d'API... 2018 a connu plusieurs failles de sécurité massives. De nouvelles cyberattaques et violations de sécurité sont signalées chaque semaine, ce qui ne contribue pas à apaiser les inquiétudes concernant les risques inhérents au cloud.

Beaucoup d'entreprises en concluent que leurs données sont plus en sécurité sur leur propre site, sur leur infrastructure cloud. En réalité, les environnements cloud hébergés sont aussi sûrs que ceux on-premises, si ce n'est plus. Ils sont conçus et entretenus par des experts de la sécurité qui connaissent le défi que représente la sécurisation du cloud et savent les relever.

Les attaques DDoS

Les attaques par déni de service (ou DDoS) représentent une inquiétude majeure pour toutes les entreprises du numérique. Au fil des années, les attaques sont de plus en plus sophistiquées et avec des nouvelles technologies comme l'Internet des objets (IoT), de nouvelles menaces apparaissent.

Une attaque DDoS surcharge un serveur web dans le but de rendre un site internet inaccessible pendant des heures ou même des jours. Cela peut provoquer une perte de revenus considérable, mais également une perte de confiance chez les clients. Une protection anti-DDoS n'est donc plus uniquement une fonctionnalité intéressante pour les entreprises, mais un système de protection crucial. Cependant, la protection sur site n'égalera jamais la capacité des systèmes leaders du marché à limiter ces attaques.

---

[1] *Source : un IDC Infobrief de juin 2019.*

« En tant que fournisseur de services cloud, nous subissons et atténuons plus de 2 000 attaques DDoS au quotidien. Notre anti-DDoS est inclus sur toutes nos offres et protège tous nos clients, pour une simple raison : si elle n'est pas atténuée, une attaque DDoS peut provoquer des dommages collatéraux. La cible ne sera donc pas la seule à subir l'attaque, mais les serveurs voisins également. Le VAC, une association de technologies développées par OVHcloud pour atténuer les attaques de ce type, ne s'active que lorsqu'une attaque est détectée. Cependant, pour nos clients qui ont des besoins en sécurité spécifiques, nous proposons un filtrage constant du trafic. En d'autres termes, une activation permanente du VAC. »

Jakub Słociński, responsable innovations réseau chez OVHcloud.

La sécurité physique et la redondance

Toutes les entreprises ne disposent pas des mêmes fonctions de sécurité physique offertes par les datacenters tiers. Cela peut créer un risque pour leurs données critiques. Un datacenter de confiance est une véritable forteresse : l'accès y est strictement surveillé et le bâtiment est protégé contre les intrusions. La vidéosurveillance et la détection de mouvement sont permanentes, ainsi que les systèmes de détection et d'extinction des incendies.

Aujourd'hui, une accessibilité constante, une haute disponibilité et une grande résilience sont les éléments fondamentaux pour de nombreux services informatiques. Atteindre le même niveau de redondance pour un cloud privé interne est une volonté ambitieuse. Dans ses datacenters, OVHcloud a mis en place une double alimentation électrique, des générateurs de secours, des systèmes d'alimentation sans interruption (ASI) et des liens réseau redondants. Construire cette infrastructure sur site implique des coûts d'achat et d'entretien élevés et nécessite un haut niveau d'expertise.

Les questions de conformité

La norme PCI DSS énumère plus de 300 contrôles et fonctions de sécurité devant être mis en place pour traiter les données de cartes bancaires en toute sécurité. Un cloud on-premises vous offre plus de contrôle sur la sécurité, mais ne facilite pas pour autant le respect des réglementations.

Assurer la mise en conformité de votre installation doit être la priorité, surtout si des données concernées par des réglementations particulières sont en jeu : numéros de cartes de paiement, informations commerciales sensibles ou données personnelles. Il s'agit d'un processus long et coûteux, nécessitant l'intervention d'un expert dans le domaine des certifications. Ce type d'activité nécessite une surveillance constante des systèmes, le développement de procédures à appliquer en cas d'incident et le chiffrage des données pour s'assurer de la permanence de la conformité.

Les problèmes de performance

La performance est une question centrale des environnements virtualisés dynamiques : difficile de prévoir la façon dont des changements sur l'infrastructure vont affecter les performances de l'application. Même une simple mise à jour logicielle peut en effet déséquilibrer un écosystème fermé.

Pour tirer le meilleur parti de votre infrastructure, il est crucial d'y intégrer un système de monitoring des performances de votre solution cloud. Pour chaque nouveau déploiement et changement de cœur, vous devez effectuer un test de performance réaliste, de préférence automatisé pour mettre en lumière les dysfonctionnements le plus tôt possible. Une fois ce processus en place, vous évitez les dépenses inutiles et pouvez surveiller de près le ratio coût-performance de votre installation.

Le surachat de ressources

Que vous construisiez votre propre cloud privé avec OpenStack ou VMware, le défi principal reste le même : comment être agile et évolutif en gérant une infrastructure en interne ? Celle-ci nécessite l'achat de plus de matériel pour augmenter sa capacité. Lorsqu'elles ne sont pas en mesure de prévoir avec précision la capacité nécessaire, les équipes informatiques achètent souvent trop de matériel pour fournir les ressources adaptées à la demande en cas de pic de charge. Par conséquent, l'entreprise se trouve face à des coûts d'investissement élevés et une capacité d'évolutivité limitée.

Peut-on pour autant parler de cloud pour qualifier une infrastructure on-premises ? Par définition, le cloud met en évidence la flexibilité et l'évolutivité sans avoir à investir dans du matériel supplémentaire. Cependant, même si beaucoup supposent que cloud privé signifie qu'il est sur site, ce n'est pas forcément le cas. Un cloud privé est une infrastructure exploitée par une seule entreprise : ses ressources sont isolées, dédiées et non mutualisées. Il permet aux entreprises de bénéficier de l'agilité nécessaire et d'augmenter leur efficacité opérationnelle tout en atténuant les risques liés à un cloud d'entreprise. Un cloud privé hébergé chez un fournisseur de services de confiance vous permet de lui confier une partie du contrôle et de la responsabilité de l'infrastructure. Ainsi, choisir un partenaire qui a fait ses preuves en matière de sécurité est essentiel pour assurer avec succès sa transition numérique.

OVHcloud est un fournisseur mondial de cloud hyperévolutif (hyperscale) qui offre aux entreprises une valeur et des performances de référence dans le secteur. Fondé en 1999, le groupe gère et entretient 30 datacenters sur quatre continents, déploie son propre réseau mondial de fibre optique et contrôle l'ensemble de la chaîne d'hébergement. S'appuyant sur ses propres infrastructures, OVHcloud propose des solutions et des outils simples et puissants qui mettent la technologie au service des entreprises tout en révolutionnant la façon dont travaillent nos plus d'un million de clients à travers le monde. Le respect des personnes, la liberté et l'égalité des chances pour l'accès aux nouvelles technologies ont toujours été des principes solidement ancrés dans l'entreprise. « *Innovation for freedom* ».