Le Cloud est-il vraiment si sûr pour nos données ?

Jadis, la cause principale des pertes de données était le vol ou la perte de bandes de sauvegarde et des ordinateurs portables… souvent oubliés sur les banquettes arrière des taxis ou dans les lieux publics !

Mais tout cela a changé lorsque les données au repos (stockées) ont été chiffrées par défaut sur les appareils portables, faisant de leur perte une simple nuisance au-delà du coût de remplacement du matériel. De fait, la technologie permettait d'atténuer un problème très humain, et cela a renforcé la tolérance aux pannes de l'entreprise. Car il n'est évidemment pas normal qu'une seule défaillance mineure, comme l'oubli d'un ordinateur portable dans une voiture, suffise à compromettre les données de toute une organisation.

Et bien, c'est exactement de ce type d'approche, de cette même tolérance aux défaillances prévisibles, dont nous avons aujourd'hui besoin dans le Cloud ! Mais nous n'y sommes malheureusement pas encore tout à fait…

L'une des raisons à cela tient au fait que nous n'avons pas toujours vraiment conscience de combien le Cloud est différent des modèles historiques auxquels nous sommes habitués.

Dans le Cloud, toute l'infrastructure est virtualisée et fonctionne comme un logiciel. Les services et les serveurs ne sont pas fixes, mais peuvent se réduire, croître, apparaître, disparaître et se transformer en un clin d'œil. D'ailleurs, on ne se pose pas vraiment la question des serveurs en tant que tels…

Et puis surtout, les services dans le Cloud ne sont pas les mêmes que ceux déployés historiquement dans les locaux de l'entreprise. Par exemple, les « *buckets* » S3 d'AWS ont des caractéristiques particulières qui relèvent à la fois du partage de fichiers et des serveurs web, tout en étant malgré tout très différents de ces modèles.

Enfin, les pratiques diffèrent également. On ne corrige pas des serveurs dans le Cloud – ils sont remplacés par les nouvelles versions des logiciels. Il existe également une distinction entre les identifiants utilisés par une instance opérationnelle (comme un ordinateur virtuel) et ceux qui sont accessibles par cette instance (les services qu'elle peut appeler, à travers des API par exemple).

L'informatique Cloud exige donc une façon distincte de penser à l'infrastructure informatique et, nécessairement, sa sécurité.

Une étude récente de l'Institut Cyentia montre que les organisations utilisant quatre fournisseurs de cloud différents ont un taux d'exposition au risque inférieur d'un quart. Les organisations qui utilisent huit fournisseurs dans le Cloud ont un taux d'exposition d'un huitième.

Ces points de données pourraient témoigner en faveur de la maturité du Cloud, de la compétence opérationnelle de ses opérateurs et de leur capacité à gérer la complexité.

Une réalité plus complexe

Mais la réalité est plus complexe. Car l'un des critères majeurs de la sécurité du Cloud est la façon dont l'entreprise va y migrer ses applications. Par exemple la stratégie de « lever et déplacer » (plus connue sous « *lift & shift* » en anglais), qui outre le fait qu'elle entraîne trop souvent des déploiements surdimensionnés et coûteux, ne corrige pas les vulnérabilités historiques présentes dans l'application.

Alors comment déterminer la bonne stratégie de migration dans le cloud pour assurer une défense optimale ?

Avant de choisir un modèle de déploiement, il est important de noter qu'il n'existe pas un environnement Cloud unique. La définition du cloud computing du National Institute of Standards and Technology (NIST) énumère trois modèles de services Cloud :

– L'infrastructure-as-a-service (IaaS)

– La plate-forme-as-a-service (PaaS)

– Le logiciel-as-a-service (SaaS)

Elle énumère également quatre modèles de déploiement : privé, communautaire, public et hybride.

Voici un bref résumé de la manière dont tout cela fonctionne dans une optique de sécurité :

Software-as-a-Service (SAAS) est un service d'application fourni par le Cloud. La majeure partie de l'infrastructure est gérée par le fournisseur. Les exemples incluent Office 365, Dropbox, Gmail, Adobe Creative Cloud, Google G Suite, DocuSign et Shopify. Ici, le client est uniquement responsable des connexions et des données. Les principales menaces sont donc le phishing, le « bourrage de mots de passe » et le vol d'identifiants.

Elles peuvent être contrôlées grâce à des solutions telles que l'authentification multifactorielle, le durcissement de la configuration des applications et le chiffrement des données au repos (si disponible) afin de limiter l'impact d'une brèche.

Platform-as-a-Service (PaaS) est une plateforme dans laquelle on peut intégrer (assembler) des applications avant qu'elles ne soient livrées par le cloud. Le fournisseur gère l'infrastructure de la plateforme, mais c'est le client qui crée et exécute les applications. Parmi les exemples de ce type d'approche, on peut citer AWS S3 buckets, Azure SQL Database, Force.com, OpenShift et Heroku. Le client n'est toujours responsable que de ses connexions et de ses données. Mais en plus des menaces liées au SaaS (attaques d'accès), il est nécessaire de sécuriser l'application elle-même contre les attaques classiques des applications web.

Dans ce modèle, il est probable que l'entreprise ait exposé des API et des interfaces de service qui pourraient contribuer à faire fuir les données si elles ne sont pas sécurisées. Les contrôles à mettre en place comprennent des processus de gestion des droits des utilisateurs/rôles, des passerelles API sécurisées, la sécurité des applications web, des pare-feux d'applications web, les détecteurs de bot et tous les contrôles SaaS référencés.

Infrastructure-as-a-Service (IaaS). Le Cloud est une plateforme permettant de construire des machines virtuelles, des réseaux et d'autres infrastructures informatiques. Le fournisseur gère l'infrastructure sous le système d'exploitation, et le client construit et exécute tout, de la machine au réseau. Les exemples incluent AWS EC2, Linode, Rackspace, Microsoft Azure et Google Compute Engine. Le client est responsable des systèmes d'exploitation, du réseau, des serveurs, ainsi que de tout ce qui se trouve dans les modèles PaaS et SaaS.

Outre les menaces visant les modèles SaaS et PaaS, les principales préoccupations en matière de sécurité sont les vulnérabilités logicielles exploitées dans les systèmes d'exploitation et les infrastructures, ainsi que les attaques de réseau. Cela nécessite un durcissement des serveurs, des réseaux et des infrastructures de services virtualisés. Il faudra donc mettre en œuvre tous les contrôles mentionnés ci-dessus, ainsi que les correctifs, un durcissement des systèmes et des contrôles de sécurité des réseaux.

On-Premises/Not Cloud est le modèle serveur traditionnel dans un rack, qu'il soit dans les locaux de l'entreprise ou dans une installation de colocation (Colo) au sein d'un datacenter. Le client est responsable de presque tout : des préoccupations liées à la connectivité et à la fiabilité du réseau, ainsi qu'à la gestion des ressources. En plus des menaces qui pèsent sur les réseaux, l'emplacement physique et le matériel, il faudra prendre en charge toutes les menaces mentionnées ci-dessus.

Dans le cadre d'un déploiement de cloud hybride, il sera nécessaire de combiner ces menaces et ces défenses. Dans ce cas, un défi supplémentaire consiste à unifier la stratégie de sécurité sans avoir à surveiller et à configurer différents contrôles, dans différents modèles et dans différents environnements.

Des compétences clés à développer pour migrer dans le Cloud

Enfin, des compétences organisationnelles spécifiques sont indispensables à développer au sein de l'entreprise afin de réduire le risque lors de la migration des applications dans le Cloud :

Compétences techniques et stratégiques

· Une bonne compréhension des technologies concernées, y compris de leurs modèles de déploiement, de leurs avantages et de leurs inconvénients sur le plan de la direction de projets et de la gestion informatique.
· Une compréhension approfondie des modes de fonctionnement et des limites des contrôles de sécurité associés.
· Une gestion complète du portefeuille de services, y compris l'environnement de suivi, les applications, les plateformes déployées et les projets informatiques en cours.
· Une capacité à évaluer les risques et modéliser les menaces, y compris la compréhension des impacts possibles des brèches et des modes de défaillance pour chaque service clé.

Processus de contrôle d'accès

· Rôles (accès et identité) clairement définis pour les utilisateurs, les services, les serveurs et les

réseaux.

· Des processus bien définis pour corriger les autorisations attribuées par erreur aux utilisateurs, ou bien les rôles erronés, obsolètes, en double ou excessifs.

· Des méthodes pour définir et modifier les règles de contrôle d'accès pour tous les éléments, services et applications de stockage de données.

· Verrouillage automatisé de l'accès à toutes les API, connexions, interfaces et nœuds de transfert de fichiers au fur et à mesure de leur mise à disposition.

· Gestion centralisée et normalisée des secrets pour le chiffrement et l'authentification.

Observabilité

· Définir et surveiller le pipeline vers la production.

· Inventaire de tous les objets, éléments de données et règles de contrôle des services dans le Cloud.

· Détection des dérives dans les configurations et audit des changements.

· Journalisation détaillée et détection des anomalies.

Respect des normes de sécurité

· Des processus pour garantir que les normes de sécurité sont choisies par défaut dans les projets, y compris les bibliothèques, *frameworks*, environnements et configurations certifiés.

· Des outils d'audit de remédiation et de gouvernance du cloud hybride.

· La correction (ou la suppression) automatisée des instances et des comptes non conformes.

· Configuration automatisée de nouvelles instances, y compris le renforcement de la sécurité selon les normes.

Toute décision stratégique et prioritaire doit passer avant les raisons technologiques. Il ne s'agit pas d'aller dans le Cloud pour le plaisir. Un objectif clairement formulé et une stratégie d'accompagnement solide montreront la voie et éclaireront les domaines où une formation et des outils plus approfondis sont nécessaires.