Stopper "Les 12 Salopards" de la sécurité

L'organisation américaine, L'Alliance de la Sécurité du Cloud (CSA), les appelle « Les 12 Salopards » qui portent atteinte à la protection des services et des applications hébergées sur le cloud.

Ceux-ci étant au moins aussi menaçants qu'Archer Maggott (aka Telly Savalas), quel que soit le surnom qu'on leur donne, il est crucial que les entreprises soucieuses de la sécurité du cloud public connaissent cette liste et prennent les mesures adéquates pour y faire face.

Certaines prédictions annoncent que dans quelques années le cloud public sera plus sécurisé que les privés - et certainement plus que les réseaux traditionnels. La sécurité devient désormais un argument de poids pour se tourner vers ce type de cloud. Toutefois, il est important de comprendre les principales préoccupations que ce dernier soulève et de séparer celles que les entreprises peuvent directement adresser de celles dont leur fournisseur est principalement responsable.

Les piratages informatiques

Le vol potentiel de données précieuses est source d'inquiétude pour toutes les entreprises ; ces craintes sont exacerbées dans les environnements de cloud ??publics car l'infrastructure de base est partagée avec d'autres locataires dont les pratiques de sécurité peuvent rendre leurs voisins vulnérables. D'ailleurs, la technologie et l'équipe du fournisseur de cloud public peuvent présenter un danger pour les clients qui ne sont pas en mesure de les contrôler. La responsabilité est donc partagée lorsqu'il s'agit d'assurer la conformité et de déployer une sécurité importante des données. Si les fournisseurs d'infrastructure et de services investissent et innovent pour renforcer les défenses, les utilisateurs doivent eux aussi s'engager pour contrôler les accès appropriés aux tâches de travail sensibles hébergées sur le cloud public.

Identifiants, références et gestion d'accès insuffisants

Les utilisateurs du cloud public peuvent utiliser les contrôles d'accès basés sur les rôles disponibles auprès du fournisseur cloud ou unifier la gestion d'identifiants en étendant la portée de ses propres systèmes. Quoi qu'il en soit, les organisations doivent veiller à ce que les informations les plus critiques ne tombent pas entre de mauvaises mains - ce qui compromettrait toutes les tâches de travail, y compris celles hébergées dans le cloud public. C'est pourquoi, la gestion des identifiants et des références doit être une priorité en termes de sécurité. Par ailleurs, la mise à jour des informations permettra d'avoir une vision claire sur les changements d'identifiants et les accès à privilège.

Des interfaces et des API dangereuses

Les fournisseurs de cloud proposent des interfaces de programmation applicative (ou API) pour permettre aux clients de personnaliser la conception et la gestion des systèmes hébergés. Toutefois, il y a un risque lié à l'utilisation des API dont l'effet de levier peut introduire des tierces parties dans le processus de programmation et de conception - créant des flux de données plus complexes. Il est vital d'avoir la capacité de surveiller continuellement ces flux afin de résoudre de potentiels problèmes et de repérer les chemins de communication suspects.

Les vulnérabilités du système

Les pirates informatiques arrivent fréquemment à s'infiltrer avec succès dans les réseaux en exploitant des systèmes non patchés, quelques secondes seulement après avoir utilisé des techniques de phishing. Les clients disposent d'un moyen simple pour éliminer certains risques associés à l'utilisation du cloud, notamment en s'assurant que tous les systèmes, y compris ceux hébergés dans le cloud public, sont corrigés et à jour.

Piratage de compte

Cette situation se produit lorsqu'une personne prend le contrôle des charges de travail fonctionnant sur le cloud public, notamment des sites web, et agit sous le nom de l'entreprise en question. Ceci est particulièrement préoccupant pour les organisations qui hébergent des services et des applications clients. En effet, outre le vol de données, le coût des contrats résiliés ou perdus et l'impact sur la réputation peuvent être énormes. Les protections contre ce type d'attaque sont similaires aux solutions évoquées dans le point numéro 2. Assurer non seulement des droits d'accès stricts, mais aussi garantir un suivi et une gestion continus de ces derniers est une priorité absolue.

Des infiltrés malveillants

La cause des brèches de sécurité du cloud public est généralement due à un employé, un travailleur indépendant ou un partenaire mécontent utilisant un accès privilégié, qui n'a pas été changé après le licenciement ou la séparation, pour infiltrer les réseaux et voler des données. Le principe d'un super-administrateur gérant toute l'infrastructure cloud pose problème car si ses identifiants sont dérobés, cela peut compromettre l'organisation sur le long terme et ouvrir de nouveaux points d'accès aux attaquants. Afin de limiter les risques, il est donc indispensable de suivre de près l'activité de ces utilisateurs privilégiés et de limiter leur accès . Si l'entreprise utilise les contrôles de son fournisseur cloud, les deux acteurs doivent mutuellement s'assurer que l'administration des accès définie est une responsabilité partagée.

Les menaces persistantes avancées (ou Advanced Persistent Threats)

Les menaces persistantes avancées ou APT utilisent le phishing et l'ingénierie sociale pour se frayer un chemin dans les réseaux et cibler des organisations qui leur rapporteront gros. Si les fournisseurs utilisent de nombreux outils sophistiqués de détection d'APT, les clients doivent également surveiller les communications dans et en dehors de leurs environnements cloud afin de s'assurer qu'ils n'ont pas été infiltrés. Un utilisateur peut tout à fait introduire un logiciel malveillant dans le cloud par inadvertance ; et bien que le fournisseur soit peut-être en mesure d'isoler ses clients, ses méthodes

ne pourront pas protéger toutes les applications de l'utilisateur infecté. C'est pourquoi des couches supplémentaires de surveillance et de contrôle d'accès sont fortement recommandées.

La perte de données

La perte totale de données précieuses fait toujours partie des préoccupations majeures lorsqu'on parle de l'hébergement sur cloud public. Bien que les pannes catastrophiques soient désormais rares, il est encore nécessaire de confirmer avec les fournisseurs que ??leurs processus ainsi que les paramètres de services du contrat assurent la sauvegarde et la récupération des informations. Si les données stockées sont particulièrement sensibles, il faudra peut-être envisager de les chiffrer, en prenant soin de protéger la clé de chiffrement et de conserver des copies à d'autres emplacements, y compris sur site.

Une due diligence insuffisante

Les organisations doivent comprendre leur niveau d'exposition en choisissant d'utiliser le cloud privé et répondre à un certain nombre de questions relatives au niveau de sécurité des données. Autant de questions qui s'inscrivent dans le cadre de la due diligence nécessaire censée idéalement précéder un projet de cloud public ; celle-ci assurera ainsi des stratégies de réponse pour chaque risque identifié.

Utilisation abusive et frauduleuse des services cloud

Le cloud public offre une puissance de calcul illimitée - constituant une véritable mine d'or pour les pirates informatiques qui en ont besoin pour les attaques par déni de service ou DDoS, la récupération d'informations et le déchiffrage de mots de passe. Il incombe principalement aux fournisseurs de services de veiller à ce que les clients utilisent leurs ressources de façon appropriée. Cependant, les locataires doivent également être vigilants et signaler toute activité suspecte ou anormale. Encore une fois, cette prudence implique l'installation d'une surveillance continue et omniprésente du trafic public hébergé dans les cloud.

Les attaques par déni de service (DDoS)

Puisque les services hébergés dans le cloud ??bénéficient d'une bonne publicité, ils sont également faciles à localiser et à attaquer. Rendre les services ou ressources d'une organisation indisponibles ou lancer des attaques low-and-slow ciblées sur des serveurs d'applications hébergeant les cloud ??n'est pas seulement coûteux en termes de pannes et de réponse lente du serveur web. Les dépenses s'ajoutent également pour l'utilisateur victime qui suite à l'attaque doit payer une plus importante puissance de calcul à son fournisseur cloud. Heureusement, ces derniers, en particulier les plus gros comme Amazon et Microsoft, ont les moyens de réduire les attaques par DDoS même à grande échelle. Toutefois, les fournisseurs plus petits n'étant pas en mesure de faire de même, le client doit élaborer un plan d'atténuation.

Technologies partagées

Le cloud permet de faire des économies sans précédent en raison de sa nature de partage. Les fournisseurs de cloud public segmentent les ressources, principalement dans le logiciel, de sorte que chacun reçoit la part dont il a besoin pour répondre aux exigences de son entreprise. Néanmoins, une segmentation inappropriée pourrait conduire à une menace unique en mesure de toucher des organisations entières. C'est pourquoi, les fournisseurs mettent en oeuvre la segmentation de l'hyperviseur et du réseau, la détection des menaces basée sur l'hôte et le réseau, ainsi que l'accès aux privilèges les plus restreints lorsqu'il s'agit de gérer l'infrastructure partagée.

Selon Gartner, le momentum et les investissements importants de la part d'acteurs tels qu'Amazon, Microsoft et Google pour rendre les cloud ??publics plus sécurisés pousseront les organisations particulièrement sensibles à les adopter. Les entreprises du secteur public, dont les enjeux de sécurité sont cruciaux, commenceront bientôt à réaliser que la plupart des fournisseurs de cloud sont mieux équipés qu'elles pour adresser les menaces qui les guettent. Ceci dit, bien que des experts et des responsables soient présents pour les accompagner, les utilisateurs d'offres de cloud publics doivent prendre conscience qu'ils sont eux-mêmes capables de passer à tabac ces « 12 Salopards », et sécuriser ainsi leurs données grâce à des technologies de visibilité. Si l'on s'en réfère au classique de Robert Aldrich, quelques salopards plus malins et débrouillards s'en sortent. Les entreprises sont prévenues, elles doivent garder une longueur d'avance !