Qu'est-ce que l'architecture de sécurité cloud ?

La sécurité cloud commence par une architecture de sécurité cloud. Une organisation doit d'abord comprendre sa posture de sécurité cloud actuelle, puis planifier les contrôles et les solutions de sécurité cloud qu'elle utilisera pour prévenir et atténuer les menaces. Cette planification est essentielle pour sécuriser les environnements hyper-complexes, qui peuvent inclure plusieurs clouds publics, services SaaS et PaaS, ressources sur site, tous accessibles à partir d'appareils d'entreprise et personnels non sécurisés.

Dans cette section, vous apprendrez :

- Pourquoi avez-vous besoin d'une architecture de sécurité cloud ?
- Modèles d'architecture de sécurité cloud
- Architecture de sécurité du cloud computing par modèle de service cloud
    - Architecture de sécurité du cloud computing IaaS
    - Architecture de sécurité du cloud computing SaaS
    - Architecture de sécurité du cloud computing PaaS

Pourquoi avez-vous besoin d'une architecture de sécurité cloud ?

À mesure que les organisations deviennent de plus en plus dépendantes du cloud, elles doivent également mettre davantage l'accent sur la sécurité. La plupart des données hors réseau transitent par des services basés sur le cloud, mais bon nombre de ces services cloud sont utilisés sans aucune planification de sécurité.

L'utilisation de fournisseurs de services cloud et de plusieurs appareils personnels complique la visualisation et le contrôle des flux de données pour les entreprises. La collaboration dans le cloud contourne les mesures de contrôle de réseau ordinaires. L'accès à des données sensibles sur des appareils personnels non gérés présente un risque majeur.

Les experts en sécurité et gestion des risques ont du mal à gagner en visibilité sur un mélange complexe d'appareils, de réseaux et de clouds. Ces mosaïques de sécurité réseau, chargées de vulnérabilités cachées, sont une invitation pour les attaquants à tenter des brèches.

De nombreux fournisseurs de services cloud ne fournissent pas d'informations détaillées sur leur environnement interne et de

nombreux contrôles de sécurité internes courants ne peuvent pas être directement convertis en cloud public.

Pour toutes ces raisons, les organisations doivent considérer la sécurité du cloud comme un nouveau défi et construire une architecture de sécurité du cloud qui les aidera à sécuriser de manière adéquate cet environnement complexe.

Modèles d'architecture de sécurité cloud

Le bon modèle peut vous aider à mettre en œuvre la sécurité dans votre organisation. Par exemple, il peut vous aider à protéger la CID (confidentialité, intégrité et disponibilité) de vos actifs de données cloud, ainsi qu'à répondre aux menaces de sécurité. Vous pouvez mettre en œuvre des contrôles de sécurité directement ou utiliser les contrôles de sécurité en tant que service proposé par votre fournisseur de cloud ou des fournisseurs tiers.

Le modèle d'architecture de sécurité cloud est généralement exprimé en termes de :

- **Contrôles de sécurité** — qui peuvent inclure des technologies et des processus. Les contrôles doivent prendre en compte l'emplacement de chaque service (entreprise, fournisseur de cloud ou tiers).

- **Limites de confiance —** entre les différents services et composants déployés sur le cloud
- **Interfaces standard et protocoles de sécurité (** tels que SSL, IPSEC, SFTP, LDAPS, SSH, SCP, SAML, OAuth, etc.)
- **Techniques utilisées pour la gestion des jetons —** authentification et autorisation
- **Méthodes de cryptage** comprenant des algorithmes tels que AES 128 bits, Triple DES, RSA, Blowfish.
- **La journalisation des événements de sécurité** -assurer tous les événements de sécurité pertinents sont capturés, hiérarchisés et remis aux équipes de sécurité.

Chaque contrôle de sécurité doit être clairement défini à l'aide des attributs suivants :

- **Fonction de** service : quel est le rôle du service ? Par exemple, cryptage, autorisation, collecte de données d'événement.
- **Emplacement logique :** service de cloud public, service tiers ou sur site. L'emplacement affecte les performances, la disponibilité, les politiques de pare-feu et la gestion des services.
- **Protocole** : quel protocole est utilisé pour accéder au service ? Par exemple, REST, HTTPS, SSH.
- **Entrée/Sortie** – qu'est-ce que le service reçoit et qu'est-ce qu'il est censé fournir ? Par exemple, l'entrée est un flux JSON et la sortie est le même flux avec des données de charge utile chiffrées.

- **Mécanismes de contrôle** : quels types de contrôle le service réalise-t-il ? Par exemple, la protection des données au repos, l'authentification des utilisateurs, l'authentification des applications.
- **Utilisateurs et opérateurs** : qui exploite ou bénéficie du service ? Par exemple, les terminaux, les utilisateurs finaux, les chefs d'entreprise, les analystes de sécurité.

Architecture de sécurité du cloud computing par modèle de service cloud

Le modèle d'architecture de sécurité cloud diffère selon le type de service cloud : IaaS (Infrastructure as a Service), PaaS (Platform as a Service) ou SaaS (Software as a Service). Ci-dessous, nous expliquons différentes considérations de sécurité pour chaque modèle.

Architecture de sécurité du cloud computing IaaS

IaaS fournit des ressources de stockage et de réseau dans le cloud. Il s'appuie fortement sur les API pour aider à gérer et à exploiter le cloud. Cependant, les API cloud ne sont souvent pas

sécurisées, car elles sont ouvertes et facilement accessibles depuis le Web.
Le fournisseur de services cloud (CSP) est responsable de la sécurisation de l'infrastructure et de la couche d'abstraction utilisées pour accéder aux ressources. Les obligations de sécurité de votre organisation couvrent le reste des couches, contenant principalement les applications métier.
Pour mieux visualiser les problèmes de sécurité du réseau cloud, déployez un Network Packet Broker (NPB) dans un environnement IaaS. Le NPB envoie le trafic et les données à un système de gestion des performances du réseau (NPM) et aux outils de sécurité pertinents. En outre, établissez la journalisation des événements se produisant sur les points de terminaison du réseau.
Les déploiements cloud IaaS nécessitent les fonctionnalités de sécurité supplémentaires suivantes :

- Segmentation du réseau
- Système de détection d'intrusion et système de prévention d'intrusion (IDS/IPS)
- Pare-feu virtuels placés devant les applications Web pour se protéger contre les codes malveillants et à la périphérie du réseau cloud
- Routeurs virtuels

Architecture de sécurité du cloud computing SaaS

Les services SaaS permettent d'accéder aux applications logicielles et aux données via un navigateur. Les termes spécifiques de la responsabilité en matière de sécurité peuvent varier d'un service à l'autre et sont parfois à négocier avec le fournisseur de services. Cloud Access Security Brokers (CASB) offre des capacités de journalisation, d'audit, de contrôle d'accès et de chiffrement qui peuvent être critiques lors de l'enquête sur les problèmes de sécurité dans un produit SaaS. De plus, assurez-vous que votre environnement SaaS possède :

- Journalisation et alerte
- Listes blanches et/ou listes noires IP
- Passerelles API, au cas où le service est accessible via l'API

Architecture de sécurité du cloud computing PaaS

Les plates-formes PaaS permettent aux entreprises de créer des applications sans la surcharge et la complexité associées à la gestion du matériel et des logiciels back-end. Dans un modèle PaaS, le CSP protège la majeure partie de l'environnement. Cependant, l'entreprise est toujours responsable de la sécurité des applications qu'elle développe.
Par conséquent, une architecture de sécurité PaaS est similaire à un modèle SaaS. Assurez-vous d'avoir CASP, la journalisation et les alertes, les restrictions IP et une passerelle API pour garantir un accès interne et externe sécurisé aux API de votre application.

Références :

https://mobidev.biz/blog/