Comment optimiser la sécurité de vos données dans Amazon Web Services

Devolutions

LA SÉCURITÉ DES DONNÉES DEVIENT UNE PRÉOCCUPATION BEAUCOUP PLUS GRANDE DANS UN ENVIRONNEMENT VIRTUEL

Les services et produits cloud Amazon (Amazon Web Services ou AWS) fournissent une plateforme infonuagique pour le stockage d'informations et le traitement de données à des millions de clients à travers monde entier, y compris les forces armées et les gouvernements. C'est l'un des plus importants fournisseurs sur le marché. Les avantages d'utiliser AWS plutôt que d'acheter des serveurs physiques peuvent sembler évidents, mais il faut rappeler que la sécurité des données devient une préoccupation beaucoup plus grande dans un environnement virtuel.

Bien qu'Amazon offre une expertise et une infrastructure en matière de sécurité, vous êtes, ultimement, l'unique responsable de la sécurité de vos données. Toute une série de mesures est nécessaire pour protéger vos données des cybercriminels, pour vous conformer aux exigences réglementaires et pour garder vos informations à l'abri du danger. Dans ce billet, nous examinerons le modèle de responsabilité partagée de la sécurité des données AWS, ainsi que certaines bonnes pratiques pour vous aider à optimiser la sécurité de vos données sur AWS.

Modèle de responsabilité partagée

Le modèle de sécurité AWS implique une responsabilité partagée entre vous et Amazon. Vous êtes responsable de l'authentification des utilisateurs, de la sécurisation de leurs accès, des systèmes d'exploitation, des applications, des réseaux et des intégrations tierces. Amazon, pour sa part, fournit une infrastructure sécurisée sous les formes suivantes :

- Outils intégrés pour créer et gérer les politiques de sécurité
- Pare-feux intégrés pour les applications Amazon Virtual Private Cloud pour la création de réseaux privés
- Connexions privées que vous pouvez activer dans des environnements locaux
- Chiffrement intégré personnalisable
- Sécurité de la couche de transport (TLS) qui fonctionne sur tous les services

AWS offre des fonctionnalités et des outils qui vous aident à sécuriser les aspects dont vous êtes responsable. Toutefois, c'est à vous de garder un œil sur les configurations de sécurité, de configurer les paramètres de manière appropriée et de gérer les accès et les privilèges accordés aux utilisateurs et aux groupes tiers. Vous pouvez trouver des explications plus détaillées sur la manière de faire ça sur le blogue de sécurité AWS.

Bonnes pratiques

Pour maximiser la sécurité, il est important de comprendre les vulnérabilités de votre configuration et de déterminer les pratiques et les solutions à appliquer pour les résoudre.

Sécurisez le contrôle des accès

D'abord, vos configurations de contrôle d'accès doivent utiliser le principe de moindre privilège (POLP), qui stipule que les droits d'accès et les autorisations sont accordés selon le principe de la nécessité. En utilisant le POLP, vous évitez que les informations d'identification compromises causent des dommages plus importants en limitant le nombre d'utilisateurs inconnus auxquels l'accès est accordé.

Aussi, il est très utile d'éviter d'utiliser l'utilisateur root après la configuration initiale d'AWS Identity and Access Management (IAM) pour s'assurer que l'accès ne soit accordé qu'aux utilisateurs approuvés.

Les services IAM vous permettent d'accorder aux utilisateurs différents niveaux d'accès aux ressources AWS et aux API. Vous pouvez limiter certains utilisateurs à la lecture seule, tout en permettant à d'autres d'accéder à toutes les fonctionnalités via des autorisations basées sur les rôles.

Lorsque vous utilisez IAM, il est important de créer des stratégies par rôle plutôt que par utilisateur. Cela vous évitera de fournir accidentellement des autorisations aux mauvais utilisateurs, tout en vous facilitant la gestion des autorisations d'utilisateur dans leur ensemble. Vous devez également éviter d'accorder des privilèges d'administrateur sauf en cas d'absolue nécessité - et toujours révoquer les privilèges lorsqu'ils ne sont plus nécessaires. Utilisez des stratégies de mots de passe forts qui empêchent les mots de passe faibles et recyclés.

Éviter la perte de données

Protéger vos données, ce n'est pas seulement d'éviter de les exposer à de potentiels cybercriminels. Il faut aussi que vos données restent intactes. Qu'elles soient dues à des attaques de logiciels malveillants, à des erreurs humaines ou à des catastrophes naturelles, la perte de données peut créer de graves problèmes financiers et de productivité. Le moyen le plus simple de vous assurer que vos données restent disponibles en tout temps consiste à les dupliquer avec des sauvegardes.

AWS propose différentes manières de sauvegarder vos données et d'éviter la perte et la corruption, que ce soit par la simple duplication de données ou en créant des instantanés Amazon EBS. Avec les instantanés, vous pouvez définir des règles dictant à quel moment les sauvegardes doivent être effectuées, combien doivent être conservées et pendant combien de temps. Cela vous aide à minimiser les risques de perte de modifications et vous offre un moyen de restaurer rapidement les éléments perdus ou corrompus.

Il est recommandé de stocker votre sauvegarde dans un emplacement différent de celui de votre service principal. En suivant la règle 3-2-1 - dans laquelle trois copies sont conservées dans deux emplacements différents, dont un hors site, vous pouvez vous assurer que même vos sauvegardes restent protégées.

Conformez-vous à la réglementation

Le respect des réglementations et des restrictions en matière de sécurité des données peut s'avérer un véritable défi. Il est important de respecter pleinement ces normes afin d'éviter des amendes substantielles et la perte de confiance des clients. Si vous pouvez éviter de stocker des informations sensibles telles que des données personnelles ou financières, faites-le. Si vous devez stocker des informations sensibles dans vos bases de données, assurez-vous que votre configuration est conforme aux normes, telles que l'utilisation du chiffrement approprié ou le respect des protocoles de suppression de données.

Bon nombre des services fournis par AWS répondent déjà aux normes de conformité communes, notamment PCI, HIPAA et RGPD. Cependant, vous devez vous assurer que votre compte respecte toutes les normes applicables. Cela inclut de rendre compte des données stockées dans les régions et les zones de disponibilité. Pour en savoir plus sur les normes et pratiques de conformité AWS, consultez le centre de conformité AWS.

Chiffrez vos données

L'un des moyens les plus simples d'éviter l'exposition de vos données consiste à chiffrer vos données. Vous devriez le faire pour les données en transit et au repos. AWS intègre des fonctionnalités de chiffrement utilisant la clé de chiffrement AES 256-bits. Vous devez toujours utiliser ces fonctionnalités, sauf si un autre service de chiffrement est disponible. La configuration spécifique varie légèrement d'un service AWS à l'autre, mais elles sont toutes assez similaires.

Si vous ne disposez pas d'un service de chiffrement externe, vous pouvez utiliser les clés gérées par le service sans frais supplémentaires. L'inconvénient de cette option est que seul le chiffrement côté serveur est activé.

Sinon, vous pouvez choisir d'utiliser le Key Management Service (KMS) offert par AWS, moyennant un coût supplémentaire. Presque tous les services AWS peuvent fonctionner avec KMS, ce qui permet de contrôler facilement les clés de chiffrement. Cela peut être fait en créant votre propre infrastructure indépendante pour le chiffrement ou en utilisant une clé principale client (CMK), définie par AWS. Si vous choisissez d'utiliser

CMK, AWS échangera votre clé principale pour vous une fois par an. Le principal avantage de l'utilisation de KMS est qu'il peut également être utilisé du côté client. Afin de maximiser la sécurité, vous devez configurer les services de chiffrement côté serveur et côté client.

Conclusion

Il y a toujours place à l'amélioration quand on parle de sécurisation des données. Néanmoins, en appliquant ces quelques pratiques simples, vous diminuerez considérablement vos chances de perdre ou de vous faire voler vos données. Rappelez-vous : restez constamment à l'affût des menaces, surveillez correctement vos données et vos configurations de sécurité et sauvegardez toutes vos données pour vous assurer qu'elles restent en sécurité et disponibles.