NumSpot
Cloud. Européen. Citoyen.

Le partenaire cloud souverain et de confiance des secteurs stratégiques et sensibles

Garantir les plus hauts standards de sécurité pour assurer la protection de leurs données et celles des citoyens.

Comment le cloud de confiance peut-il aider les entreprises à prévenir les violations de données et à réduire les risques de sécurité ?

Résumé

- Le **cloud de confiance** (qualifié SecNumCloud par l'ANSSI) offre une protection renforcée contre les violations de données et diminue les risques de sécurité pour les entreprises.
- Pour **prévenir les risques de sécurité** dans le cloud, les entreprises doivent adopter des **mesures de sécurité avancées**, notamment en suivant les étapes clés nécessaires pour éviter le piratage, les pertes de données, les erreurs de configuration et les violations de conformité.
- Cette solution permet de stocker et gérer les données en accord avec **les lois et réglementations européennes**, garantit une meilleure **sécurité des données sensibles** et surtout prémunit **contre les lois extraterritoriales**.

Le cloud computing a révolutionné la manière dont les entreprises stockent et gèrent leurs données. Cependant, avec cette nouvelle technologie viennent également de nouveaux défis en matière de sécurité de ces données : les entreprises doivent notamment s'assurer que leurs données sont protégées contre les cyberattaques et leur violation potentielle.

La notion de cloud de confiance offre ici une solution pour **prévenir les violations de données** et réduire les risques, car du point de vue de l'entreprise, une violation de données peut aussi être le résultat d'un accès non voulu à celles-ci par un agent ou une entité sous le coup d'une injonction d'un état non européen. **A fortiori, le cloud de confiance souverain est la solution ultime.**

Les risques potentiels de sécurité dans le cloud et comment vous pouvez les prévenir

Lorsqu'il s'agit de sécurité dans le cloud, il est important d'identifier les risques potentiels et de mettre en place les mesures de prévention adéquates.

1 Attaques par piratage

Les attaques par déni de service distribué (DDoS) par exemple, ou encore le phishing et l'injection de code, peuvent compromettre la sécurité des données stockées dans le cloud. Pour prévenir ces attaques, mettez en place des mesures de sécurité avancées, pare-feu, systèmes de détection d'intrusion...

2 Pertes de données

Celles-ci peuvent survenir en raison de défaillances matérielles, de logiciels défectueux ou de mauvaises pratiques de sauvegarde. Pour vous en prémunir, vous pouvez mettre en place des sauvegardes régulières et de tester régulièrement leur fonctionnalité pour s'assurer qu'elles sont efficaces.

3 Erreurs de configuration

Les erreurs de configuration, telles que la mauvaise configuration des paramètres de sécurité et des stratégies de partage de fichiers, peuvent ouvrir la porte à des violations de sécurité. Pour les prévenir, vous pouvez miser sur des politiques de sécurité claires et de former les employés aux bonnes pratiques en matière de sécurité informatique.

4 Violations de conformité

Elles conformité surviennent lorsque les entreprises ne respectent pas les réglementations et normes en matière de sécurité des données. Pour les éviter, il est essentiel que vous vous assuriez que les politiques de sécurité sont conformes aux réglementations locales et industrielles et de mettre en place des mécanismes de surveillance et de contrôle pour garantir leur respect.

Étapes clés pour la sécurité de vos données cloud

Pour garantir la sécurité de vos données dans le cloud, voici **8 étapes clés à suivre** :

1 Déployer une réplication des données

Effectuer des copies de sauvegarde de vos données est essentiel pour prévenir les pertes de données en cas d'incident majeur. Il est recommandé d'opter pour une réplication des données dans plusieurs datacenters, idéalement situés dans des régions différentes, et ainsi d'assurer la disponibilité des données en toutes circonstances.

2 Assurer le chiffrement de bout en bout

Celui-ci est capital pour assurer la confidentialité et la sécurité des données échangées dans le cloud. Il est recommandé d'opter pour un cloud de confiance qui propose un chiffrement de bout en bout, aussi bien au niveau de l'envoi que du stockage des données.

3 Recourir à la double authentification

C'est une mesure de sécurité très efficace pour vérifier l'authenticité des connexions aux données cloud, vous pouvez la mettre en place en demandant notamment à l'utilisateur de fournir un mot de passe et de valider son identité à l'aide d'un code envoyé sur son téléphone portable.

4 Définir une stratégie de gestion des droits d'utilisateur

La gestion des droits d'utilisateur est toute aussi importante pour limiter l'accès aux données sensibles et réduire les risques de vol ou de divulgation non autorisée : il est recommandé que vous limitiez l'accès aux données en fonction des besoins et des responsabilités des utilisateurs.

5 Renforcer la sécurité des données sensibles

Certaines données sensibles nécessitent une protection renforcée et pour celles-ci il est recommandé d'utiliser des mots de passe supplémentaires, des alertes de téléchargement ou de transfert de données sensibles, ainsi que de mettre en place des mesures de surveillance pour détecter toute activité suspecte.

6 Demande de qualification

Les ransomwares sont une menace croissante pour la sécurité des données dans le cloud. Il est alors recommandé d'utiliser une solution anti-ransomware qui bloque les requêtes DNS provenant de sites malveillants et protège vos données contre les attaques de ransomware.

7 Automatiser les mises à jour applicatives

Effectuer des copies de sauvegarde de vos données est essentiel pour prévenir les pertes de données en cas d'incident majeur. Il est recommandé d'opter pour une réplication des données dans plusieurs datacenters, idéalement situés dans des régions différentes, et ainsi d'assurer la disponibilité des données en toutes circonstances.

8 Choisir des services cloud souverains

Celui-ci est capital pour assurer la confidentialité et la sécurité des données échangées dans le cloud. Il est recommandé d'opter pour un cloud de confiance qui propose un chiffrement de bout en bout, aussi bien au niveau de l'envoi que du stockage des données.

Pour protéger les données sensibles et **prévenir les conséquences financières** et réputationnelles néfastes en cas de violations de données, il est essentiel de vous prémunir contre ces risques. Le choix d'un **cloud de confiance** vous offre ainsi une solution fiable pour **garantir la sécurité des données** et **assurer la conformité** avec les réglementations en vigueur.

Les enjeux de sécurité du cloud et la nécessité d'une approche souveraine

La transition numérique des entreprises les expose à des **risques juridiques** et **financiers**, voire **stratégiques** en optant pour des acteurs cloud non-européens et non qualifiés.

L'utilisation d'un service cloud implique que les entreprises confient leurs données à un tiers dont elles attendent aussi qu'il garantisse la confidentialité et la sécurité de ces données.

SecNumCloud

Dans le cas du **cloud souverain et de confiance**, les données sont stockées dans des **centres de données situés en France et en Europe**, sont soumises aux **lois et réglementations européennes** en matière de protection des données et protégées par les plus **hauts standards de sécurité**.

À propos de NumSpot

NumSpot est un acteur du cloud souverain et de confiance. Né de la volonté de 4 entreprises françaises de premier plan des secteurs public et privé (Banque des Territoires, Docaposte, Dassault Systèmes et Bouygues Télécom), NumSpot propose une offre de cloud indépendant, souverain et robuste adossé au IaaS d'OUTSCALE qualifié SecNumCloud. NumSpot est un cloud réversible et transparent, basé principalement sur l'open source et des solutions européennes. L'offre NumSpot s'adresse prioritairement aux secteurs confrontés à une forte sensibilité des données (secteur public, santé, services financiers et assurance, OIV et OSE) en France et en Europe, et à la recherche d'une solution souveraine et de confiance en accord avec les règlementations RGPD et européennes. NumSpot fait ainsi le choix d'œuvrer pour l'intérêt général en proposant un véritable pacte de confiance entre un fournisseur de cloud, ses clients et les citoyens européens.

Suivez-nous @NumSpot @NumSpotCloud